MIRAPOINT

a CP company

RazorSafe Software Configuration Guide

Release 5.2
December 2012
Part Number 010-00865c

This manual supports Archive Operating System (AOS) releases 5.2 and later AOS releases until replaced by a newer edition.

OTHER THAN ANY EXPRESS LIMITED WARRANTIES THAT MIRAPOINT PROVIDES TO YOU IN WRITING, MIRAPOINT AND MIRAPOINT'S LICENSORS PROVIDE THE SOFTWARE TO YOU “AS IS” AND EXPRESSLY DISCLAIM ALL WARRANTIES AND/OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MIRAPOINT'S LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (INCLUDING NEGLIGENCE OR OTHER TORT), ARISING IN ANY WAY OUT OF YOUR USE OF THE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF DAMAGES. MIRAPOINT’S LIABILITY SHALL BE AS LIMITED IN THE LICENSE AGREEMENT.

Contents

C

D

Preface

The Mirapoint RazorSafe Configuration Guide provides Archive Operating System (AOS) software configuration procedures for all RazorSafe appliances, regardless of the hardware model. This manual also includes procedural information on how to backup and restore emails and logs from a remote server.

This manual assumes that you are familiar with industry-standard networking concepts and terminology and have a general understanding of how Internet email messaging works.

This manual provides information on the following installation and configuration tasks:

Chapter 1, Getting Started: Introductory information about the RazorSafe architecture and how to configure IP addresses on the RazorSafe appliance.

Chapter 2, Configuring Mirapoint Message Server for RazorSafe Archiving: How to configure Mirapoint Message Server for archiving.

Chapter 3, Configuring Microsoft Exchange Server for RazorSafe Archiving: How to configure Microsoft Exchange Server 2000/2003 for archiving.

Chapter 4, Configuring IBM Lotus Domino for RazorSafe Archiving: How to configure IBM Lotus Domino server for archiving.

Chapter 5, Completing the RazorSafe Configuration: How to complete the RazorSafe appliance configuration, including post-configuration administrative tasks.

Appendix A, Configuring SAN Storage: How to configure a S7000-RS appliance to work with a supported SAN storage solution.

Appendix A, Using RazorSafe Backup and Restore: How to backup and restore emails and logs from a supported remote host.

Appendix B, Performing a System Recovery of a RazorSafe Appliance: How to resintall AOS from a System Recovery CD and perform a restore of your appliance.

Appendix C, Expanding Message Storage Capacity for Mirapoint Message Servers: How to expand the message storage capacity on the RazorSafe appliance for use with a Mirapoint Message Server.

About Mirapoint Documentation

Documentation for all Mirapoint products is available through the Information Library on the Mirapoint Support website:

https://support.mirapoint.com/

The Information Library provides the hardware and software documentation for all supported Mirapoint releases and appliances, and the Support Knowledge Base. The Support site is accessible to all customers with a valid Support Contract. If your company has a valid contract but you need a Support login ID, email support@mirapoint.com.

For a glossary of terms associated with Mirapoint products, see http://www.mirapoint.com/glossary/.

Getting Technical Support

If you experience problems with your appliance, contact the company from which you purchased your Mirapoint appliance.

If you purchased your appliance directly from Mirapoint, contact Mirapoint Technical Support by email, telephone, or via the Mirapoint Support website:

Email: support@mirapoint.com
(China) support@mirapoint.com.cn

Telephone:

(USA) 1-877-MIRAPOINT (1-877-647-2764)

(UK) +44 (or 0) 1628-535699

(China) 400 707 1086

(Australia) 1 800 633 784

(Elsewhere) +1 408-720-3800

Website: https://support.mirapoint.com/

When contacting Technical Support, be prepared with the following information about your appliance:

Table 1 Appliance Information for Technical Support

Information	MOS CLI command (Message Server, RazorGate)	AOS UI Location (RazorSafe)
Software release	`Version`	In the Status tab, select System Info.
Host ID	`License Hostid`	In the Status tab, select System Info.
Serial number	`Model Get Serial`	In the Status tab, select System Info.
Hardware model	`Model Get Chassis`	In the Status tab, select System Info.

Typographic Conventions

Table 2 describes what the different fonts and typefaces indicate in this manual.

Table 2 Typographic Conventions in This Manual

Typeface	Use	Example
Bold	User interface elements	From the File menu, select Save As...
Italic	Definitions, emphasis, or titles	A folder is a container that stores email messages. Specify at least two DNS servers. For more information, see the Mirapoint Message Server Administrator's Guide.
`Courier`	Screen display text, command names, or text to type *	`Enter your IP address:` Use the `License Hostid` command. At the prompt, type `Version`.
`Courier Italic`	Variables for which you substitute when you type	*`your_IP_address`*

* Command-line interface (CLI) commands are case-*in*sensitive, except where noted. For readability, commands in this manual are shown in mixed case (for example, `License Hostid`).

Iconic Conventions

Table 3 describes what the different icons in this manual indicate.

Table 3 Iconic Conventions in This Manual

Icon	Use
💡	Best practices information (Mirapoint recommendations)
➡	Note information that should be read
❗	Critical information
🔑	License information
⚡	Potential of causing bodily harm (hardware only)

1

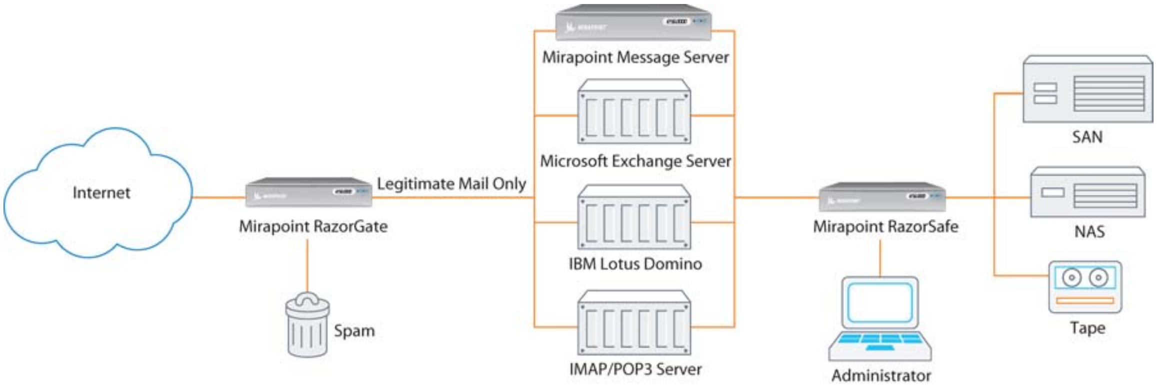
Getting Started

This chapter includes conceptual information regarding RazorSafe architecture and the archival process, as well as procedural steps on how to assign IP addresses to the appliance and a supported email server (e.g., Mirapoint Message Server, Microsoft Exchange Server, etc.) using the RazorSafe console.

Understanding RazorSafe Archiving

RazorSafe passively and discretely copies all messages sent or received within an organization, indexes them, and places them into a specified archive. The appliance integrates easily into any existing Mirapoint Message Server and RazorGate solution but supports, and is capable of communicating with, a variety of email servers over the network (see Figure 1).

Figure 1 RazorSafe Architecture Overview



Messages from an email server are stored on the RazorSafe's local disk drives or on a Storage Area Network (SAN) and can then be archived to either a remote server via CIFS/SMB, NFS, or SCSI protocols (on Network Attached Storage (NAS), SAN, file server, etc.).

If you are using SAN storage device, then using your filer's backup or snapshot utilities is an approved backup method.

RazorSafe's search capabilities allow users to discover messages based on sender, recipient, subject, keyword, date range, and other criteria. All actions by users, administrators, or by the appliance itself are recorded in a secure audit log. For more information, see the RazorSafe online help.

Mirapoint recommends reading through the Mirapoint Support Knowledge Base, accessible from the Mirapoint Support website, for additional RazorSafe information.

Deployment Procedure

In order to properly deploy a RazorSafe appliance within your environment, you must complete the following configuration tasks:

Make sure that you have completed the instructions in the Mirapoint RazorSafe 7-Series Hardware Getting Started Guide before beginning this procedure.

1. Assign an IP address to the RazorSafe appliance. For more information, see Assigning IP Addresses on page 13.
2. Configure your email server for RazorSafe archiving. For more information, see the appropriate section for your supported email server:

   Configuring Mirapoint Message Server for RazorSafe Archiving on page 15

   Configuring Microsoft Exchange Server for RazorSafe Archiving on page 21. This includes procedures for Exchange 2000/2003 and 2007/2010.

   Configuring IBM Lotus Domino for RazorSafe Archiving on page 39
3. Complete the configuration on the RazorSafe appliance:

   a. (For Mirapoint S7000-RS Appliances Only) Make sure you have properly set up and configured your SAN storage device. For more information, see Configuring SAN Storage on page 49.

   b. Set up the RazorSafe to get email from the email server. For more information, see Finishing the RazorSafe Configuration on page 43.

   – If you are running Exchange 2007/2010, and are sending journal messages to a valid, enabled mailbox, you must configure an IMAP fetcher.

   – If you are running Exchange 2007/2010, and are sending journal messages to a mailbox-enabled contact, you do not need to configure an IMAP fetcher and can proceed to configure additional configuration options on the RazorSafe and verify the overall environment. For more information, see Additional RazorSafe Configuration Options on page 45 and Verifying RazorSafe Message Archiving on page 47.

c. Verify that messages are downloading successfully to the RazorSafe. For more information, see Additional RazorSafe Configuration Options on page 45.

d. Create user accounts and configure additional options. For more information, see Additional RazorSafe Configuration Options on page 45.

e. (Optional) Install any necessary email client tools. For more information, see Installing and Using Email Client Tools on page 47.

Assigning IP Addresses

The RazorSafe appliance and email server (e.g., Mirapoint Message Server, Microsoft Exchange Server, etc.) must be network-connected before you can begin configuration. By default, RazorSafe obtains its IP address dynamically from the DHCP (Dynamic Host Configuration Protocol) server. If your site has a DHCP server, you could use it to assign an IP address to the RazorSafe appliance, but this is not recommended.

Mirapoint recommends assigning the IP address manually, so it always remains the same, regardless of DHCP service.

To assign IP addresses properly for the RazorSafe, complete the following steps:

1. Obtain a previously unassigned IP addresses for the RazorSafe.
2. Assign the new IP address to the RazorSafe by following the procedure given in Manually Assigning an IP Address (Console) on page 13.

Once set, if you alter the RazorSafe's IP address, you must reboot the appliance to make the change effective.

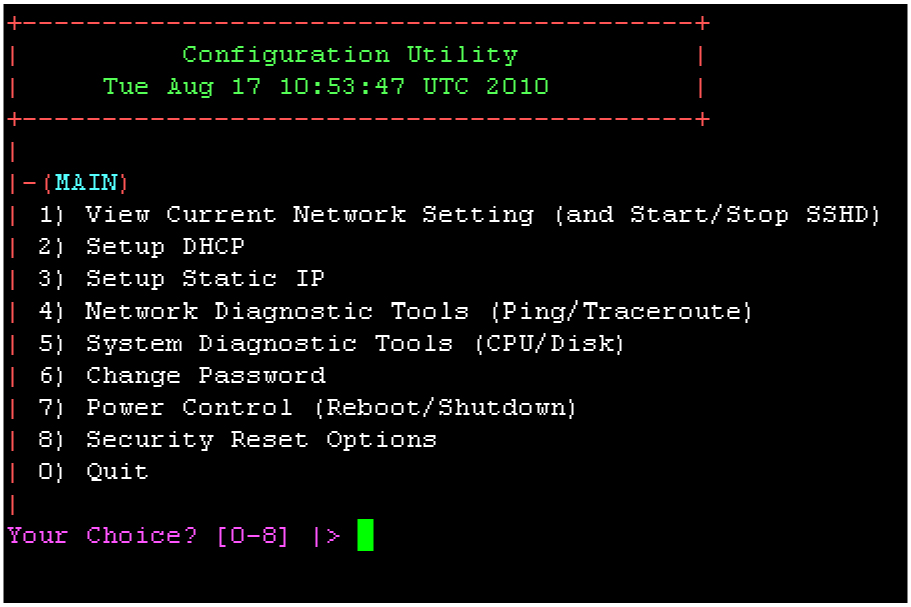
Manually Assigning an IP Address (Console)

To manually assign an IP address to the RazorSafe, you must have a VGA monitor and PC keyboard, then complete the following steps:

1. Connect the monitor cable to the VGA monitor input. Also connect a PC keyboard to the USB socket. For more information, on see the Mirapoint RazorSafe 7-Series Hardware Getting Started Guide.
2. In the console, log in as administrator `miradmin`, with password `ChangeMe` at the prompt.

   After login, the configuration utility appears.

Figure 2 Configuration Utility



```
+-------------------------------------------+
|         Configuration Utility             |
|     Tue Aug 17 10:53:47 UTC 2010          |
+-------------------------------------------+
|
|-(MAIN)
| 1) View Current Network Setting (and Start/Stop SSHD)
| 2) Setup DHCP
| 3) Setup Static IP
| 4) Network Diagnostic Tools (Ping/Traceroute)
| 5) System Diagnostic Tools (CPU/Disk)
| 6) Change Password
| 7) Power Control (Reboot/Shutdown)
| 8) Security Reset Options
| 0) Quit
|
Your Choice? [0-8] |>
```

3. Choose option `3`, `Set up Static IP`.
4. Next, if you plugged the ethernet cable into port 0, choose `1` (`eth0`).
5. At the prompt, type in the following information:

   IP address assigned to the RazorSafe

   The prevailing netmask, such as 255.255.0.0

   Default gateway for this subnet; the first few octets should be the same as for the RazorSafe's IP address

   Fully-qualified domain name (FQDN) of the RazorSafe

   IP address of a DNS server (i.e., Nameserver)
6. Type `y` to confirm your changes.
7. Finally, choose option `1` to review all the network settings.

Make sure you follow the procedures in this manual for your respective email server. For more information, see Next Steps, Configuring the Email Server on page 14.

Next Steps, Configuring the Email Server

Once you have assigned an IP address to a RazorSafe, you must configure your email server for RazorSafe archiving. For more information, see the appropriate section for your supported email server:

Configuring Mirapoint Message Server for RazorSafe Archiving on page 15

Configuring Microsoft Exchange Server for RazorSafe Archiving on page 21

Configuring IBM Lotus Domino for RazorSafe Archiving on page 39

2

Configuring Mirapoint Message Server for RazorSafe Archiving

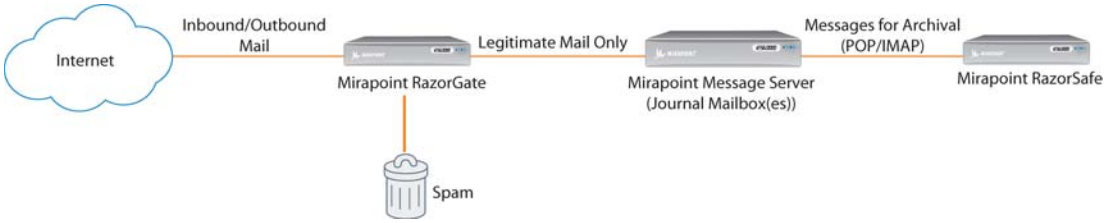
This chapter provides procedures on how to create a new user account and mail folder, and set up the required mail filters on a Mirapoint Message Server. This user account, mail folder, and mail filters are necessary in order for the RazorSafe to properly archive emails from the Message Server.

Understanding RazorSafe Archiving on a Message Server

At specified time intervals, the RazorSafe logs into journal mailboxes (i.e., user folders) on the Message Server in order to collect messages for indexing. Once the messages are indexed and archived, the original messages are deleted from the journal mailbox, completing the archival process.

Mirapoint appliance policy control and filtering capabilities allow administrators to capture both inbound and outbound messages and organize the archive by sender, recipient, department or keyword. Also, Mirapoint appliances (e.g., RazorGate) can dramatically decrease the percentage of junk mail (i.e., spam) going into the archive by blocking that mail at the edge of the network, before it ever reaches the Message Server (see Figure 3).

Figure 3 Message Server, RazorGate, and RazorSafe Communication



This manual does not include information on RazorGate features, functionality, or configuration. For more information on RazorGate appliances, see the Mirapoint Hardware Guide for your appliance model, the Mirapoint MOS Configuration Guide, and the Mirapoint RazorGate Administrator's Guide.

Configuring a Message Server

You can use either the Administration Suite or the command-line interface (CLI) to configure the Message Server:

Using Administration Suite to Configure a Message Server on page 16

Using the CLI to Configure a Message Server on page 19

Using Administration Suite to Configure a Message Server

To configure the Message Server using the Administration Suite, complete the following steps:

1. Open a web browser, then type in the following URL:

   `http://mirasys/miradmin`

   Where *mirasys* represents the Message Server's IP address or hostname.

2. Log in as `Administrator` using the password you specified for the Message Server during its hardware setup.

3. Verify the Message Server's license.

   To verify licenses, navigate to the Home > System > Utilities > License page and review the list of licenses for this appliance.

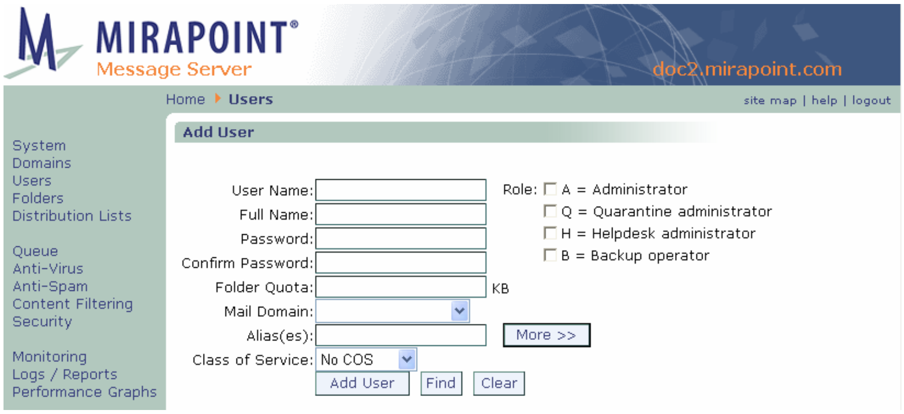
4. Verify that the appropriate service (i.e., POP, IMAP, etc.) is enabled and started.

   To verify the service, navigate to Home > System > Services and select the page for the service you want to enable and start. If the service is disabled, click Enable it. If the service is stopped, click Start it.

5. Navigate back to the Home page, and click Users.

   The Add User page displays.

Figure 4 Add User Page



Class of Service: No COS

6. Add a new user account by populating the fields as indicated in Table 4 below, then click Add User.

Table 4 Add User Parameters

Add User Field	Value Definition
User Name	Type in a username (for example, `journalmailbox`)
Full Name	Type in the full name of the user (for example, `Journal Mailbox`)
Password	Type in the desired password
Confirm Password	Re-type the password
Folder Quota	Leave this field blank
Mail Domain	Type in the domain name where this user is to reside (for example, `mirapoint.example.com`)
Alias(es)	Leave this field blank.
Class of Service	This field displays only if LDAP GUI is configured. Select No COS from the drop-down menu.
Role	Leave this unselected

Do not use LDAP or LDAP autoprovisioning to create the *`journalmailbox`* user account.

If the message count in the user account you just created exceeds the 150K message limitation, see Expanding Message Storage Capacity for Mirapoint Message Servers on page 59 for information on expanding the number of user accounts to accommodate the higher message volume.

7. Create a wiretap content filter to direct a copy of all messages to the RazorSafe.

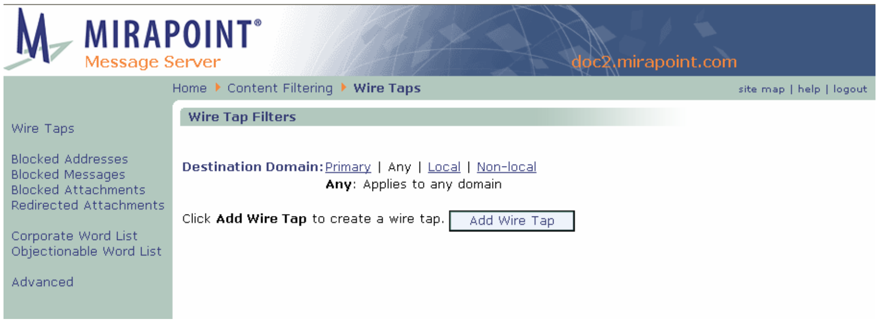
Before creating the wiretap filter, make sure the destination account (see step 4 on page 16) exists. The destination account should not have quota or autoreply set, otherwise, you might experience problems which can bring down the Message Server.

To create the content filter (wiretap), complete the following steps:

a. Navigate to the Home > Content Filtering > Wire Taps page.

The Wire Tap Filters page displays.

Figure 5 Wire Tap Filters Page



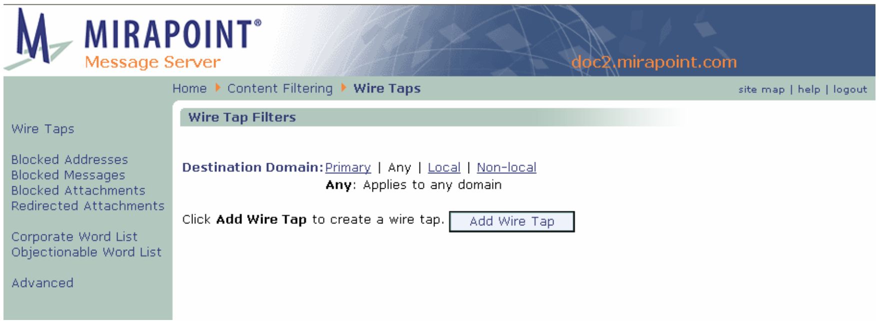
Any: Applies to any domain

Click **Add Wire Tap** to create a wire tap.

b. Select Any for the Destination Domain (see Figure 5), then click Add Wire Tap.

The Add/Edit Wire Tap Filter page displays.

Figure 6 Add/Edit Wire Tap Filter Page



Any: Applies to any domain

Click **Add Wire Tap** to create a wire tap.

c. Populate the following fields as indicated in Table 5, then click OK.

Table 5 Add/Edit Wire Tape Filter Parameters

Wire Tap Filters Field	Value Definition
Address to Wire Tap	Type an asterisk (*) to indicate “any”
Forward to	Type the name of the new user you created in step 4 on page 19, (for example, `journalmailbox`).

For more information on how to configure a Message Server using the Administration Suite, see the Mirapoint MOS Configuration Guide, and the Mirapoint Message Server Administrator’s Guide or the Administration Suite online help.

Once you have completed your Message Server configuration, you must complete the RazorSafe configuration. For more information, see Completing the RazorSafe Configuration on page 43.

Using the CLI to Configure a Message Server

To configure the Message Server using the CLI, complete the following steps:

1. Log in to the CLI as follows:
   a. Using a telnet client, connect to the default telnet port (port 23) on the Message Server. You can identify the appliance using the IP address you assigned to it.
   b. Log in as `Administrator` using the password you specified for the Message Server during its hardware setup. For example:

      ```
      OK mail.example.com admind 4.1 server ready

      User: Administrator
      Password: password
      OK User logged in
      mail.example.com
      ```

2. Verify that Message Server is licensed using the `License List` command. In the following example, the third response line displays the license for the service. (In this example POP is licensed.)

   ```
   License List "" "" ""

   * ie78aiHhn93 "User-limit unlimited" ""
   * dF+MrP2WHUf "Upgrades Allowed" ""
   * nzdCi2dZZ98 "POP unlimited users" ""
   * bzaG14emPS8 "Group calendar unlimited users" ""
   * 2voVS8r6PXb "Message Server" ""
   OK Completed
   ```

3. Check if the service (i.e., POP, IMAP, etc.) is enabled and started using the following commands:

   ```
   Service Enabled Service

   Service Started Service
   ```

   Where *`Service`* is the service name. For example,

   ```
   Service Enabled Pop

   Service Started Pop
   ```

   If the service is not enabled or started, you must enable and start it using the following commands:

   ```
   Service Enable Service

   Service Start Service
   ```

4. Create a new user account using the following commands:

   ```
   User Add journalmailbox “Journal Mailbox” password

   Mailbox Add user.journalmailbox
   ```

   Where *`journalmailbox`* is the username, *`Journal Mailbox`* is the full name of the user, and *`password`* is the desired password for the user.

   If the message count in the user account you just created exceeds the 150K message limitation, see Expanding Message Storage Capacity for Mirapoint Message Servers on page 59 for information on expanding the number of user accounts to accommodate the higher message volume.

5. Create a wiretap content filter to direct a copy of all messages to the RazorSafe.

Before creating the wiretap filter, make sure the destination account (see step 4 above) exists. The destination account should not have quota or autoreply set, otherwise, you might experience problems which can bring down the Message Server.

Use the following command and filter string:

```
Filter Add (Domain=any) rsTap Wiretap "(To=journalmailbox)" Allof Continue
.
```

The third argument, rsTap, is the (arbitrary) name of this filter. You must complete the filter command with a period (.) on a line by itself.

For more information on how to configure a Message Server using the CLI, see the Mirapoint MOS Configuration Guide, and the Mirapoint Administration Protocol Reference or CLI online help.

Next Steps, Completing the RazorSafe Configuration

Once you have created a user, mail folder, and content filter on the Message Server, you must complete the RazorSafe configuration. For more information, see Completing the RazorSafe Configuration on page 43.

3

Configuring Microsoft Exchange Server for RazorSafe Archiving

This chapter includes procedural steps on how to configure Microsoft Exchange Server 2000/2003 and 2007/2010 for RazorSafe archiving.

Understanding Journaling on Exchange Server

Microsoft Exchange uses a feature named journaling to create a copy of all email communications within a single Exchange mail store or Exchange organization. These email copies are sent to a dedicated mailbox on an Exchange server.

Archiving is a different process than journaling. Archiving is a means of storing the email copies in a different environment, such as the RazorSafe.

The following journaling types within Exchange are supported by RazorSafe:

Message-only Journaling (Exchange 2000/2003 only)—Creates a copy of all messages and the email header data to and from users on a mailbox database and sends the message copy to a specified mailbox (called the journal recipient).

This method of journaling does not capture Blind Carbon Copy (Bcc) recipients, nor does it expand distribution list recipients. In a regulatory compliance situation this journaling method would not satisfy those requirements and thus should not be used.

Envelope Journaling (Exchange 2000/2003 and 2007/2010)—Envelope journaling archives transport envelope (i.e., P1 message header) information, this includes recipients who actually received the message (including Bcc recipients and recipients in distribution lists). The original message appears as an attachment, with the body of the journal report (not the X-Sender/X-Receiver headers) containing the recipient information.

Bcc Journaling is only captured using Envelope Journaling. For more information on Bcc journaling, see your Microsoft product documentation.

Envelope Journaling is enabled on Exchange 2000/2003 only after specific Service Packs (SPs) are applied. However, for Exchange 2007/2010, Envelope Journaling is the only method available for Exchange 2007/2010 users in a 2007/2010 native environment.

Mirapoint recommends using Envelope Journaling when configuring Exchange 2000/2003 for RazorSafe archiving. For more information, see Enabling Journaling on Exchange Server 2000/2003 on page 26.

Exchange does not support journaling on public folders. Therefore, email posts to public folders cannot be archived to the RazorSafe.

Exchange Server 2000/2003 Standard Edition vs. 2000/2003 Enterprise Edition

How you set up journaling depends on your environment and the version and edition of Exchange that you are running. Exchange 2000/2003 is available in Standard Edition and Enterprise Edition:

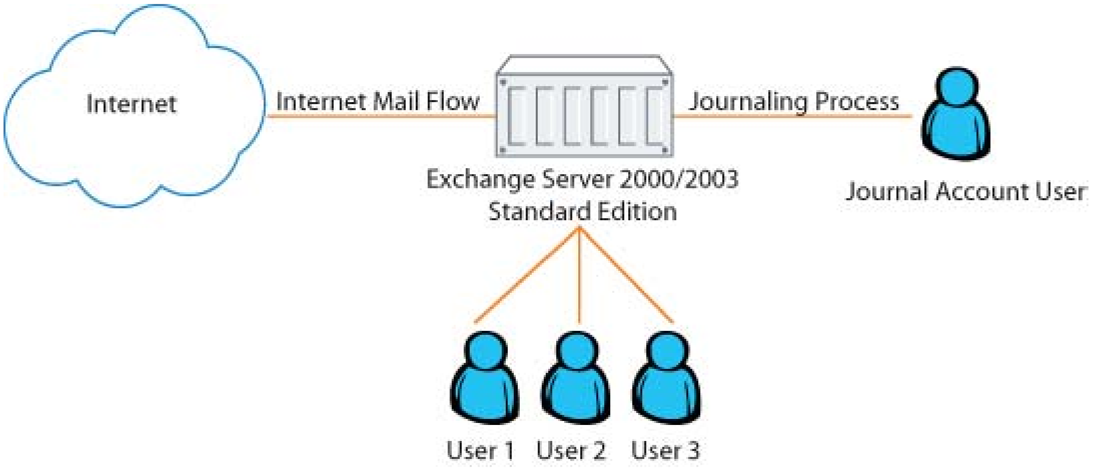
Standard Edition—Contains only one mail store, therefore the journal mailbox recipient must reside on the same mail store as the rest of your users, unless there is more than one Exchange server in your organization.

Enterprise Edition—Multiple mail stores can be created, limited only by your storage space. Individual mail stores can be selected for journaling, and the journal account can reside on any one of those mail stores. This is useful for selectively enabling or disabling journaling for specific users.

Standard Edition Deployment Example

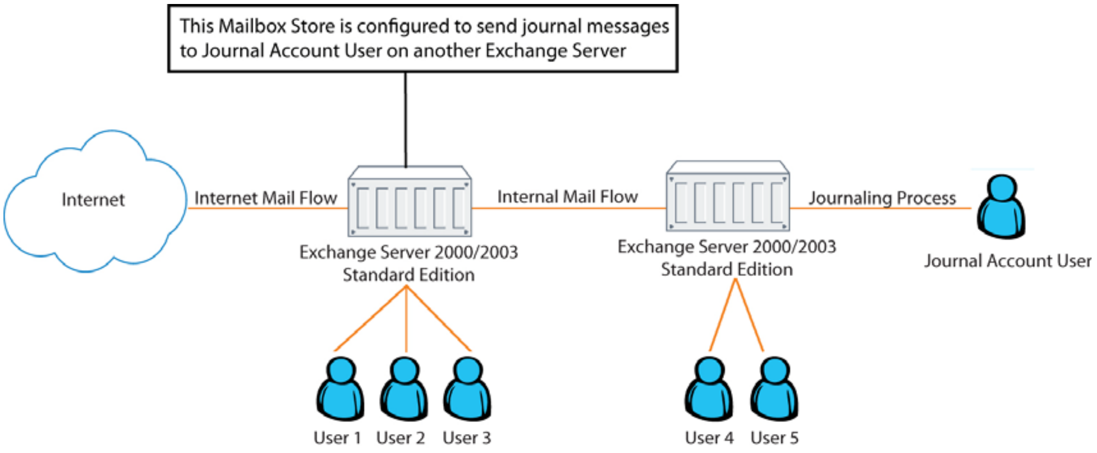
Standard Edition only allows for one mail store per server. In a single Exchange server environment the configuration is limited to enabling journaling on the main Exchange server (see Figure 7).

Figure 7 Single Standard Edition Server - Multiple Users and Journal Account User



Alternatively, if you had multiple servers running Standard Edition, you could choose which server contained the journal mailbox (see Figure 8).

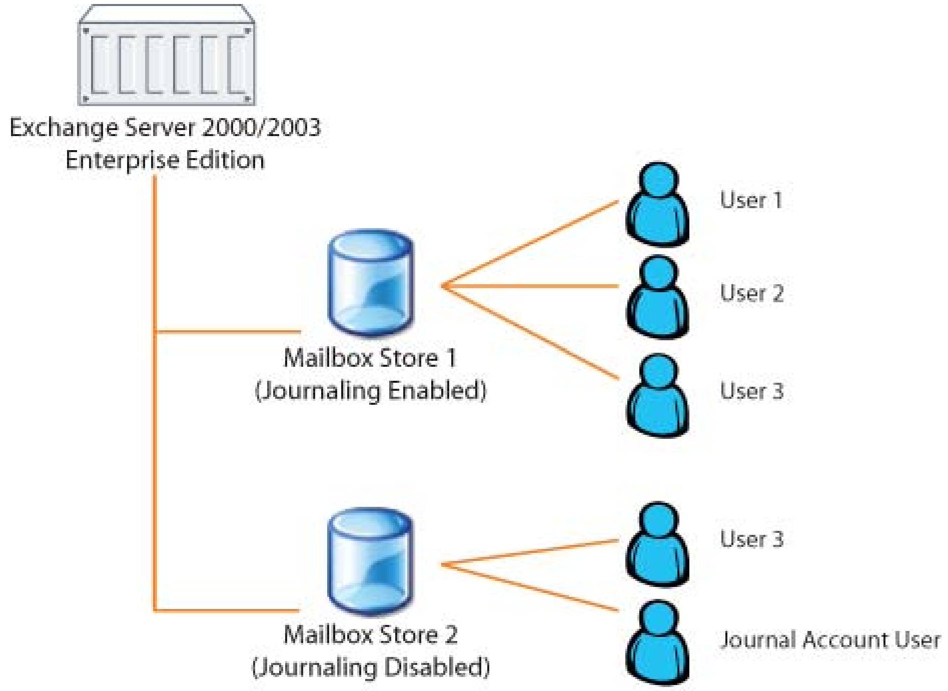
Figure 8 Multiple Standard Edition Servers - Multiple Users and Journal Account User Located on Another Mail Store


This Mailbox Store is configured to send journal messages to Journal Account User on another Exchange Server
Internet
Internet Mail Flow
Internal Mail Flow
Journaling Process
Exchange Server 2000/2003
Standard Edition
Exchange Server 2000/2003
Standard Edition
Journal Account User
User 1
User 2
User 3
User 4
User 5

Enterprise Edition Deployment Example

Enterprise Edition allows for multiple mail stores on a single server. Journaling works much the same here as with Standard Edition, with the exception that you can select which mail stores are enabled for journaling. This allows you to select certain users to be included or excluded from the journaling process.

Figure 9 Enterprise Edition Server - Multiple Mail Stores with Journaling Enabled on a Per-Store Basis



In this particular deployment example, you want to avoid using two different journal accounts for each server. You do not want to get into a situation where messages could be journaled or copied twice.

So, in the example detailed in Figure 9, two different journaling accounts are used, if `User 1` emails `User 4`, the account specified for journaling on `Mailbox Store 1` will get a copy of the message, and the account specified for journaling on `Mailbox Store 2` will copy the message. Also, messages on `Mailbox Store 2` are not journaled.

Regardless of the edition or deployment method used, enabling journaling can increase the load on your Exchange server anywhere between 15% to 33%, according to Microsoft. Therefore you might want to set tighter restrictions on users' email storage quotas or implement system policies to restrict the message durations for which these users can store messages on the mail store. By doing so, you can off-set the increased load that journaling places on Exchange. For more information, see the Microsoft product documentation at: http://technet.microsoft.com/en-us/library/aa997525.

This chapter provides procedural information on how to enable journaling on Exchange 2000/2003 Standard and Enterprise Edition. For more information, see Enabling Journaling on Exchange Server 2000/2003 on page 26.

Exchange Server 2007/2010

With Exchange 2007, journaling makes use of the role-based topology in Exchange. All messages are processed by Hub Transport servers, from mailbox and unified messaging servers, other Exchange servers (including legacy 2000/2003 servers), and the Internet. All messages are handled through a Hub Transport server, and every Hub Transport server contains a transport agent, called the Journaling Agent.

The Journaling Agent evaluates every message before delivering it to the final recipient. The agent can be configured to journal messages from a specific user or group of users. It can also be configured to journal a specific scope of messages, such as internal messages which capture only internal message traffic, external messages where the sender or one of the recipients is outside of the Exchange server, and global messages which includes both internal and external message categories.

If you are running Exchange 2007/2010 with Standard Client Access Licenses (CALs), you can use per-mailbox store journaling. However, if you want to use per-recipient journaling you must use the Enterprise CALs.

Sending Journal Reports

With Exchange 2007/2010, you can specify a mailbox recipient or send the journal reports (i.e., messages) directly to the RazorSafe. Regardless, you must create a recipient object within Microsoft Active Directory. The recipient can be a mailbox, a mail-enabled contact that redirects the mail to the RazorSafe, or a distribution list that contains both mailboxes and/or contacts.

Also, be sure to include the size and physical locations of your Exchange servers when considering how and where to send the journal reports. Journaling can result in a significant number of repetitive reports. According to Microsoft, the added overhead is approximately 15%.

If you are running a mixed Exchange 2007/2010 and 2000/2003 environment, you must have the 2000/2003 server house the journal mailbox. This is necessary due to how Exchange determines if a message needs to be sent to the journal mailbox. If you place the journal mailbox on the 2007/2010 server, you will cause multiple journal reports to be sent to the journal recipient.

There are certain cases where multiple journal reports are created, regardless of your environment’s configuration:

Addresses include individual recipients and a distribution group. In this case, a journal report of the message is created for individual recipients, and another for the distribution group.

The number of addresses exceeds the chipping size. In this case, the message is bifurcated so that each copy meets the size requirement, so each copy is journaled.

With Exchange 2007 Service Pack (SP) 1, if a message includes a distribution group and the message is delivered to a Hub Transport Server that does not function as the expansion server for that distribution group, the message is forwarded to the appropriate expansion server and both Hub Transport Servers will journal the message.

This chapter provides procedural information on how to enable journaling on Exchange 2007/2010 Standard and Enterprise Edition. For more information, see Enabling Journaling on Exchange Server 2007/2010 on page 27.

Enabling Journaling on Exchange Server 2000/2003

This section provides procedural information on how to enable journaling on Exchange 2000/2003 Standard and Enterprise Edition.

System Requirements

Prior to enabling journaling, Mirapoint recommends reading Exchange Server 2000/2003 Standard Edition vs. 2000/2003 Enterprise Edition on page 22.

Exchange Server 2000 requires Service Pack (SP) 3, along with a hotfix for Envelope Journaling. For more information, see the Microsoft Support Knowledge Base (http://support.microsoft.com/kb/870540).

Exchange Server 2003 requires SP 2.

To enable Envelope Journaling on Exchange 2000/2003, you must download the Microsoft Exchange Server Email Journaling Advanced Configuration tool (`exejcfg.exe`) available from the Microsoft Download Center (http://www.microsoft.com/downloads/en/default.aspx).

Enabling Journaling Using Microsoft Exchange System Manager (ESM)

To enable journaling using ESM, complete the following steps:

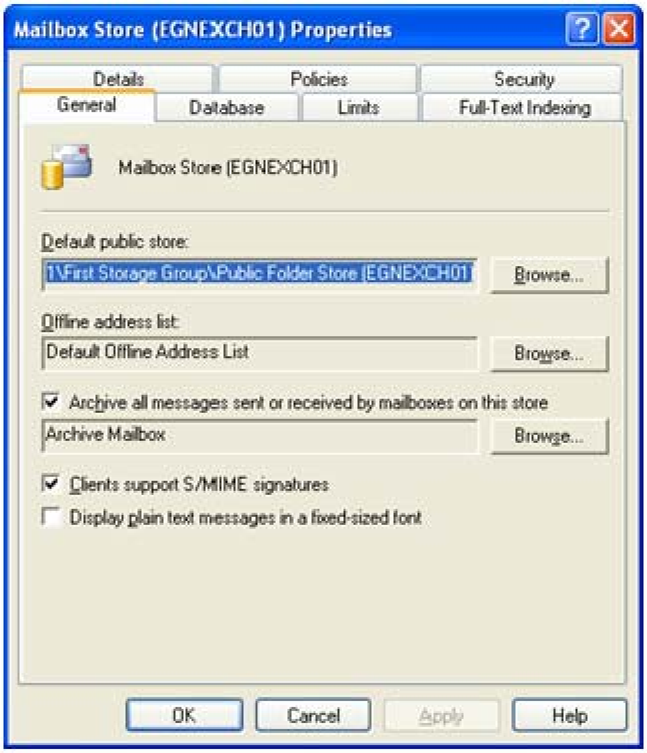
1. Within the Windows Microsoft Management Console (MMC), access the Active Directory Users and Computers snap-in and create a mail-enabled user to send the journal messages to.
2. Open ESM and expand the Servers list.
3. Open the appropriate server displayed within the list.
4. Under First Storage Group locate the entry named Mailbox Store.

In Exchange 2000/2003 Enterprise Edition the storage group names might be different depending on your organization's naming conventions.

5. Right-click on Mailbox Store and select Properties.
6. Within the Mailbox Store Properties window, select the General tab.
7. On the General tab, select the Archive all messages sent or received by mailboxes on this store checkbox.

8. Click Browse to select the mailbox user you created for the archive in step 1.

Figure 10 Mailbox Store Properties Window



Mailbox Store (EGNEXCH01) Properties

Mailbox Store (EGNEXCH01)

Default public store: 1\First Storage Group\Public Folder Store (EGNEXCH01

Offline address list: Default Offline Address List

☑ Archive all messages sent or received by mailboxes on this store

Archive Mailbox

☑ Clients support S/MIME signatures

☐ Display plain text messages in a fixed-sized font

9. Click OK.

Enabling Envelope Journaling in Exchange 2000/2003

Envelope Journaling is not enabled by default. In order to enable Envelope Journaling you must use the Microsoft Exchange Server Email Journaling Advanced Configuration tool. For detailed instructions on the tool, see the Microsoft product documentation.

Enabling Journaling on Exchange Server 2007/2010

This section provides procedural information on how to enable journaling on Exchange 2007/2010 Standard and Enterprise Edition.

System Requirements

Prior to enabling journaling, Mirapoint recommends reading Exchange Server 2007/2010 on page 25.

Exchange Server 2007 (Service Packs (SPs) 1 and 2 are not required)

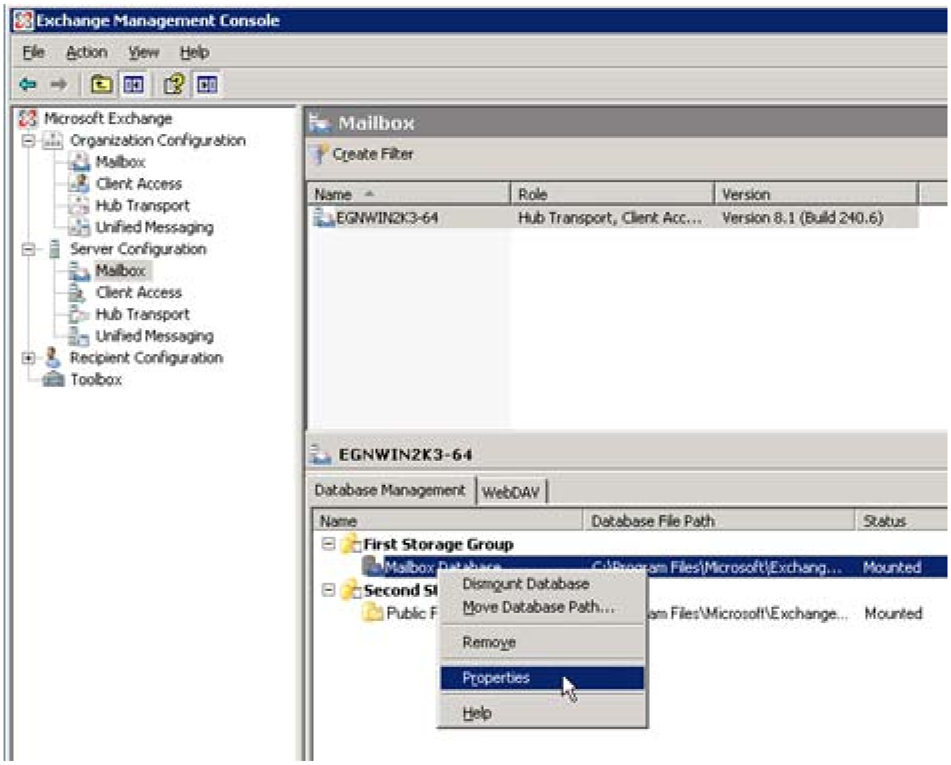
Exchange Server 2010

Enabling Mailbox Database Journaling in Exchange 2007

The Mailbox Database Journaling feature was removed in Exchange 2010. This procedure only applies to Exchange 2007, however, if you want to enable journaling in 2007 using journal rules instead, see Creating and Enabling Journal Rules in Exchange 2007/2010 on page 29.

To enable journaling on an entire mailbox store, complete the following steps:

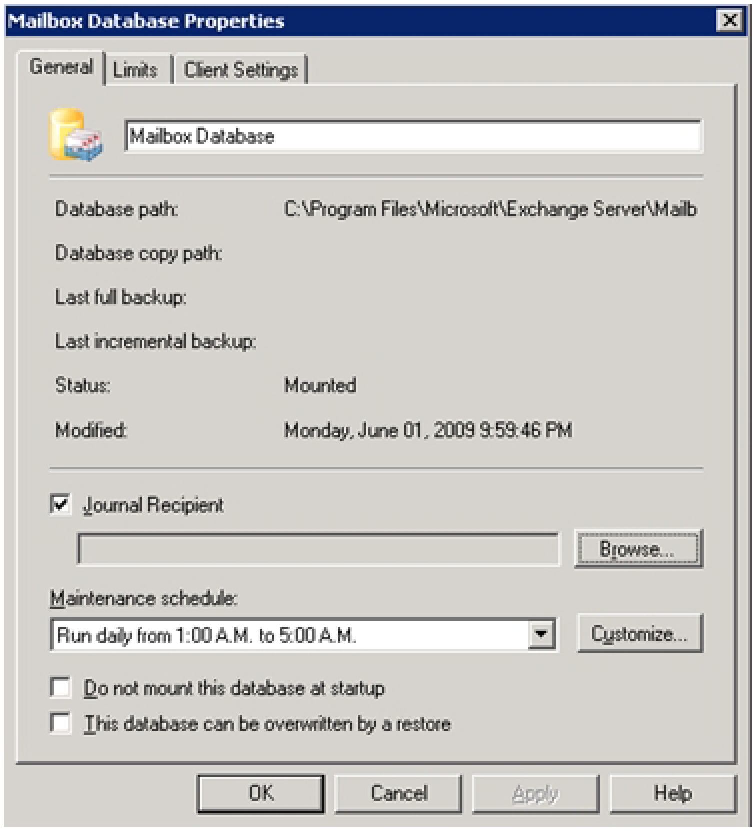
1. Open the Exchange Management Console (EMC) and go to Server Configuration > Mailbox in the navigation tree.
2. Right-click on the Mailbox Database and select Properties from the menu.



Name	Role	Version
EGNWIN2K3-64	Hub Transport, Client Acc...	Version 8.1 (Build 240.6)

Name	Database File Path	Status
First Storage Group		
Mailbox Database	C:\Program Files\Microsoft\Exchang...	Mounted
Second St		
Public F	am Files\Microsoft\Exchange...	Mounted

The Mailbox Database Properties window appears.



Mailbox Database

Database path: C:\Program Files\Microsoft\Exchange Server\Mailb

Database copy path:

Last full backup:

Last incremental backup:

Status: Mounted

Modified: Monday, June 01, 2009 9:59:46 PM

☑ Journal Recipient

Maintenance schedule: Run daily from 1:00 A.M. to 5:00 A.M.

☐ Do not mount this database at startup

☐ This database can be overwritten by a restore

3. On the General tab, select the Journal Recipient checkbox, then click Browse to select mailbox/contact you want the journal reports (i.e., messages) sent to.
4. Click Ok.

Creating and Enabling Journal Rules in Exchange 2007/2010

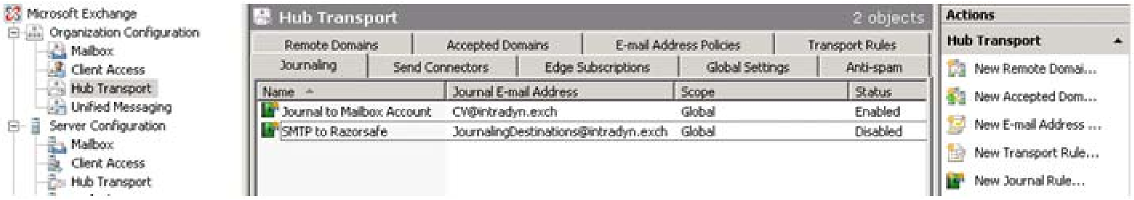
In Exchange 2010, or in Exchange 2007 with Enterprise Client Access Licenses (CALs), you can create journal rules within the scope of the organization.

If you have already enabled Mailbox Database Journaling for Exchange 2007, you do not need to complete this procedure. For more information, see Enabling Mailbox Database Journaling in Exchange 2007 on page 28.

To create and enable journal rules, complete the following steps:

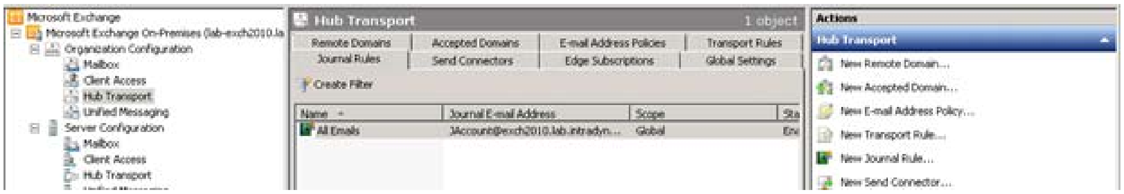
1. Open the Exchange Management Console (EMC) and go to Organization Configuration > Hub Transport in the navigation tree.
2. Click the Journaling tab in Exchange 2007 or the Journal Rules tab in Exchange 2010.

Figure 11 Journaling Tab - Exchange 2007



Name	Journal E-mail Address	Scope	Status
Journal to Mailbox Account	CV@intradyn.exch	Global	Enabled
SMTP to Razorsafe	JournalingDestinations@intradyn.exch	Global	Disabled

Figure 12 Journal Rules Tab - Exchange 2010

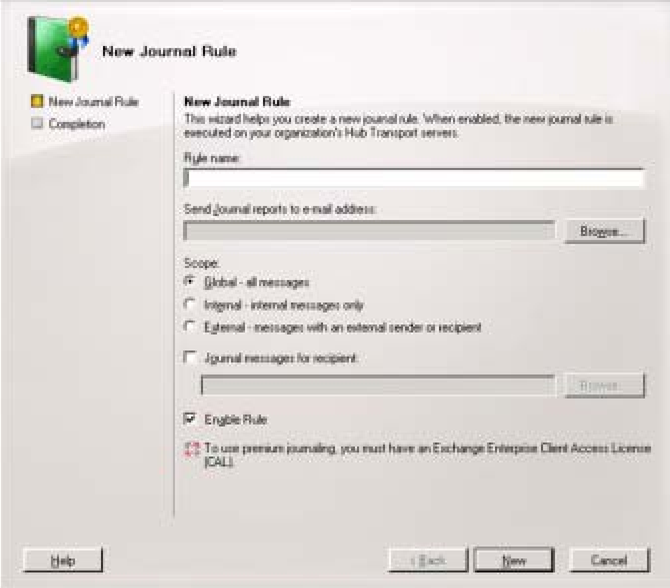


Name	Journal E-mail Address	Scope	Sta
All Emails	JAccount@exch2010.lab.intradyn...	Global	En

The procedure for creating a journal rule in Exchange 2010 is exactly the same as Exchange 2007. The remainder of the procedure will refer to the user interface in Exchange 2007 only.

3. In the Actions page, click New Journal Rule. (You can also right-click in the tab.)

   The New Journal Rule window appears.



New Journal Rule

This wizard helps you create a new journal rule. When enabled, the new journal rule is executed on your organization's Hub Transport servers.

Rule name:

Send Journal reports to e-mail address:

Scope:

● Global - all messages

○ Internal - internal messages only

○ External - messages with an external sender or recipient

☐ Journal messages for recipient:

☑ Enable Rule

To use premium journaling, you must have an Exchange Enterprise Client Access License (CAL).

4. In the Rule Name text field, type in a name for the rule.
5. For the Send Journal Reports to e-mail address option, click Browse to specify the mailbox recipient that the messages will be sent to (i.e., a valid, enabled mailbox or a mailbox-enabled contact).

If you specify a mailbox, you must configure an IMAP fetcher on the RazorSafe after you complete this procedure. For more information, see Finishing the RazorSafe Configuration on page 43.

If you specify a mailbox-enabled contact, you can send journal messages directly to the RazorSafe. A fetcher is not required. For more information, see Sending Journal Messages to a Mailbox-enabled Contact on page 31.

6. (Optional) If you select the Journal messages for recipient checkbox, you can enable journaling for an individual user or you can choose a security/ distribution group to enable journaling for multiple users. Selecting this option allows you to create different journal rules for different members of the organization.
7. Click New.

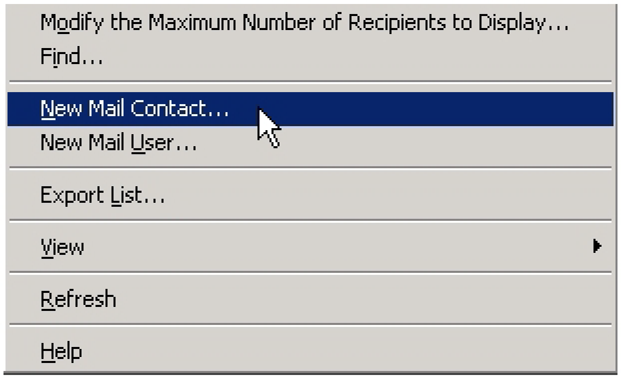
Sending Journal Messages to a Mailbox-enabled Contact

While creating journal rules in Exchange you can choose to send messages to a specific mailbox or to a mailbox-enabled contact (see Creating and Enabling Journal Rules in Exchange 2007/2010 on page 29, step 5). If you chose a specific mailbox, you do not need to complete the following procedure.

Choosing a mailbox-enabled contact allows you to send messages directly to the RazorSafe. So, storing emails and attachments twice on the Exchange server is unnecessary, saving disk space and improving network utilization. However, if communication between the RazorSafe and Exchange's Hub Transport is disrupted for any reason, messages will build up rapidly in the queue.You will need to decide which method (i.e., mailbox or mailbox-enabled contact) works best for your organization.

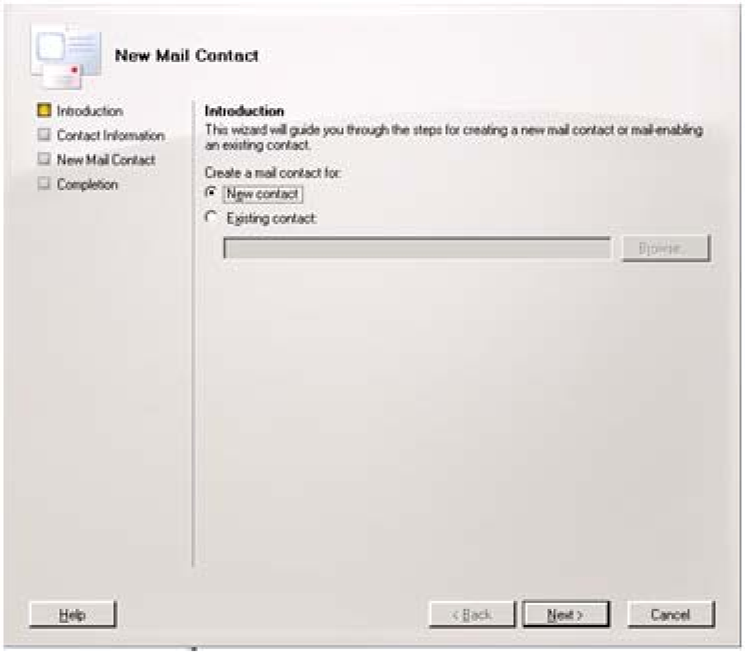
If you decide to configure Exchange to send messages via a mailbox-enabled contact directly to the RazorSafe (as opposed to specifying a mailbox), then you must complete the following steps after completing the procedure described in Creating and Enabling Journal Rules in Exchange 2007/2010 on page 29:

1. Open the Exchange Management Console (EMC) and go to Recipient Configuration in the navigation tree and make sure that section is expanded.
2. Right-click Mail Contact and select New Mail Contact.



The New Mail Contact window appears.

3. On the Introduction page, create a new contact or use an existing contact record to mail-enable. Select the option works best for your environment and click Next.



New Mail Contact

Introduction

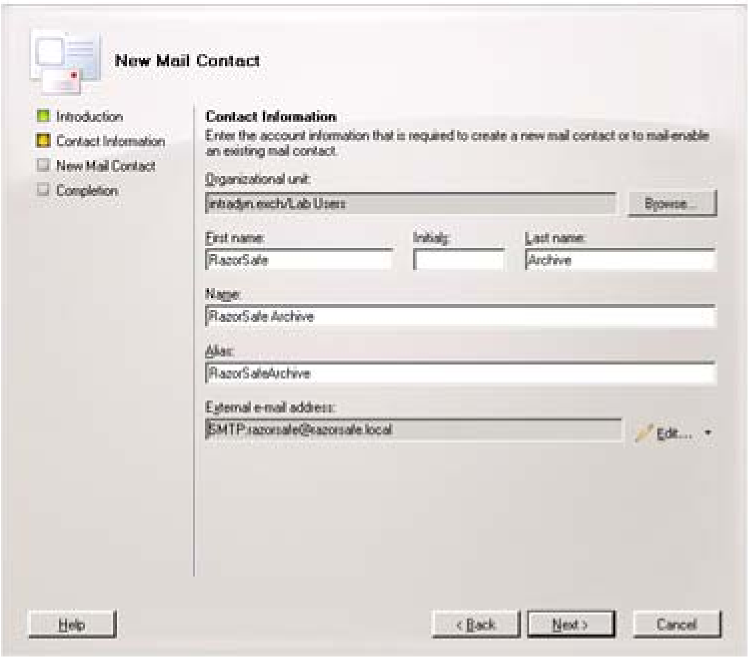
This wizard will guide you through the steps for creating a new mail contact or mail-enabling an existing contact.

Create a mail contact for:

● New contact

○ Existing contact

4. On the Contact Information page, create a contact record that has a primary SMTP address that is invalid (e.g., `xyz@company.local`, `xyz@company.lab`, etc.). In this example, `SMTP.razorsafe@razorsafe.local` is used:



New Mail Contact

Contact Information

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

Organizational unit: intradyn.exch/Lab Users

First name: RazorSafe

Initials:

Last name: Archive

Name: RazorSafe Archive

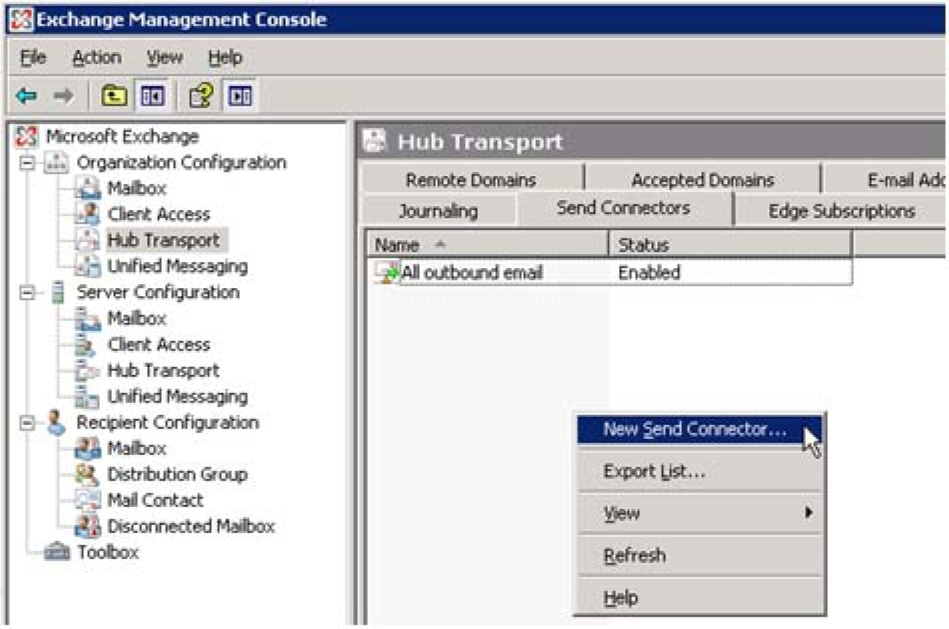
Alias: RazorSafeArchive

External e-mail address: SMTP:razorsafe@razorsafe.local

5. Click Next and finish creating the contact.

   In the following steps, you will create an Exchange Send Connector that will tell the Hub Transport how to handle these journal messages.

6. In the left pane of the EMC window, navigate to Organization Configuration > Hub Transport in the navigation tree.
7. On the Send Connectors tab, right-click and select New Send Connector.

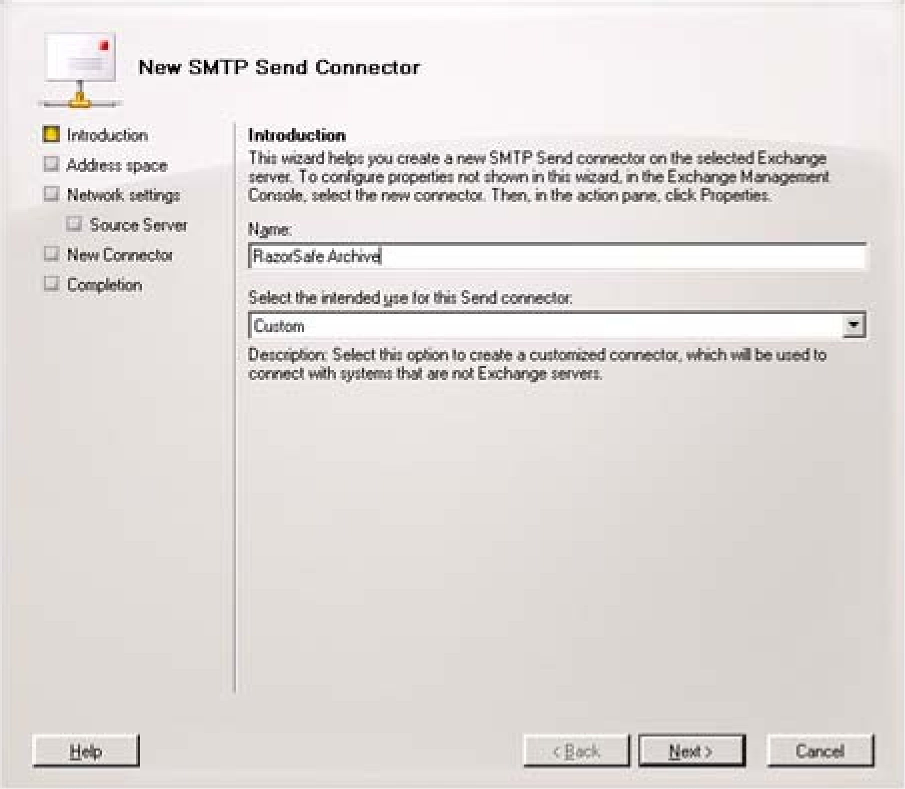


Name	Status
All outbound email	Enabled

The New SMTP Send Connector window appears.

8. On the Introduction page, complete the following steps:
   a. Type in a Name for the connector in the text field.
   b. From the Select the intended use for this Send connector drop-down menu, select Custom.
   c. Click Next.

Figure 13 New SMTP Send Connector - Introduction



Introduction

This wizard helps you create a new SMTP Send connector on the selected Exchange server. To configure properties not shown in this wizard, in the Exchange Management Console, select the new connector. Then, in the action pane, click Properties.

Name: RazorSafe Archive

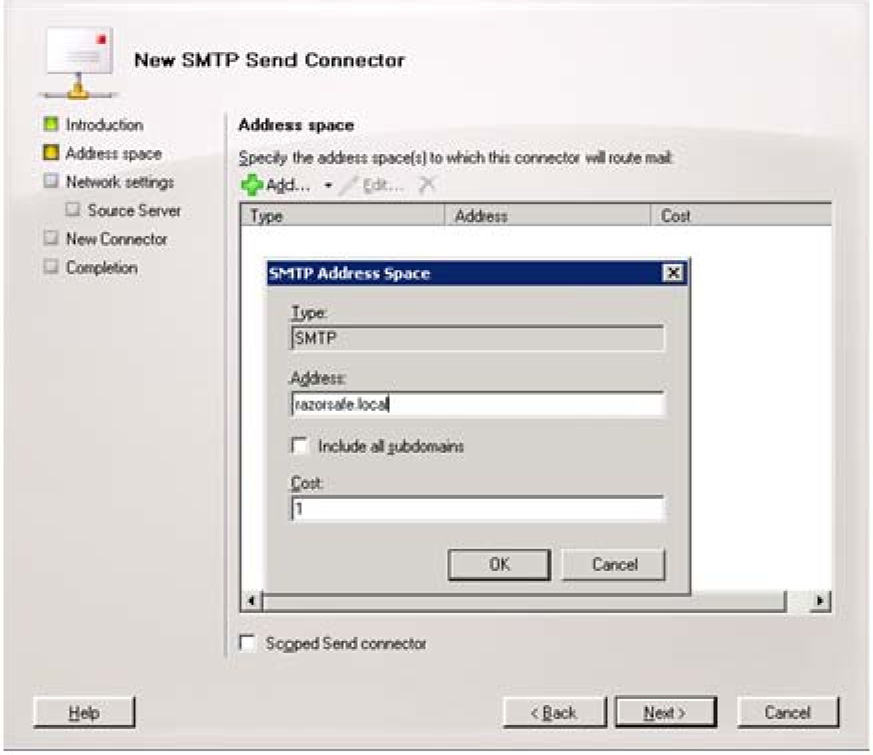
Select the intended use for this Send connector: Custom

Description: Select this option to create a customized connector, which will be used to connect with systems that are not Exchange servers.

9. On the Address space page, complete the following steps:
   a. Click Add.

      The SMTP Address Space window appears.
   b. For the Address text field, type in whatever invalid email domain you created in step 4. In this example, `razorsafe.local` is used:
   c. Click OK.
   d. Click Next.

Figure 14 New SMTP Send Connector - Address Space



Address space

Specify the address space(s) to which this connector will route mail:

Type: SMTP

Address: razorsafe.local

☐ Include all subdomains

Cost: 1

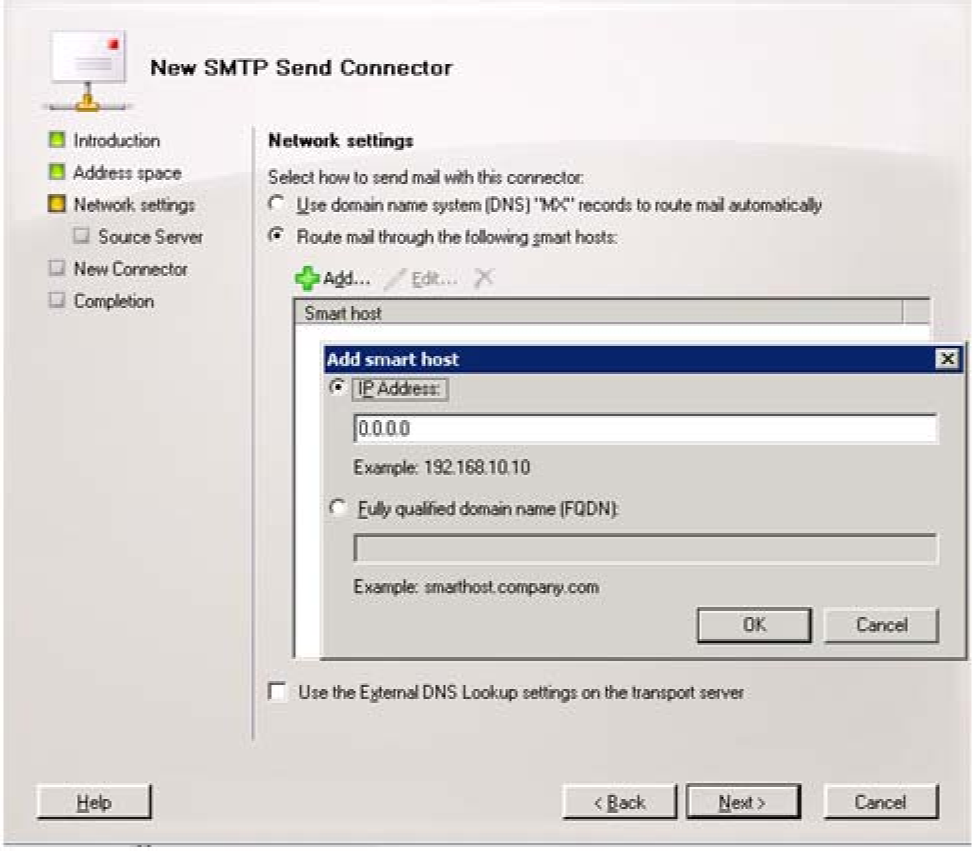
☐ Scoped Send connector

10. On the Network settings page, complete the following steps:
    a. Select the Route mail through the following smart hosts radio button.
    b. Click Add.

       The Add smart host window appears. The SMTP Send Connector is where you want to specify the RazorSafe IP address.

    c. Select the IP Address radio button and type in the IP of the RazorSafe.
    d. Click OK.
    e. Click Next.

Figure 15 New SMTP Send Connector - Network Settings



Network settings

Select how to send mail with this connector:

○ Use domain name system (DNS) "MX" records to route mail automatically

● Route mail through the following smart hosts:

Smart host

Add smart host

● IP Address:

0.0.0.0

Example: 192.168.10.10

○ Fully qualified domain name (FQDN):

Example: smarthost.company.com

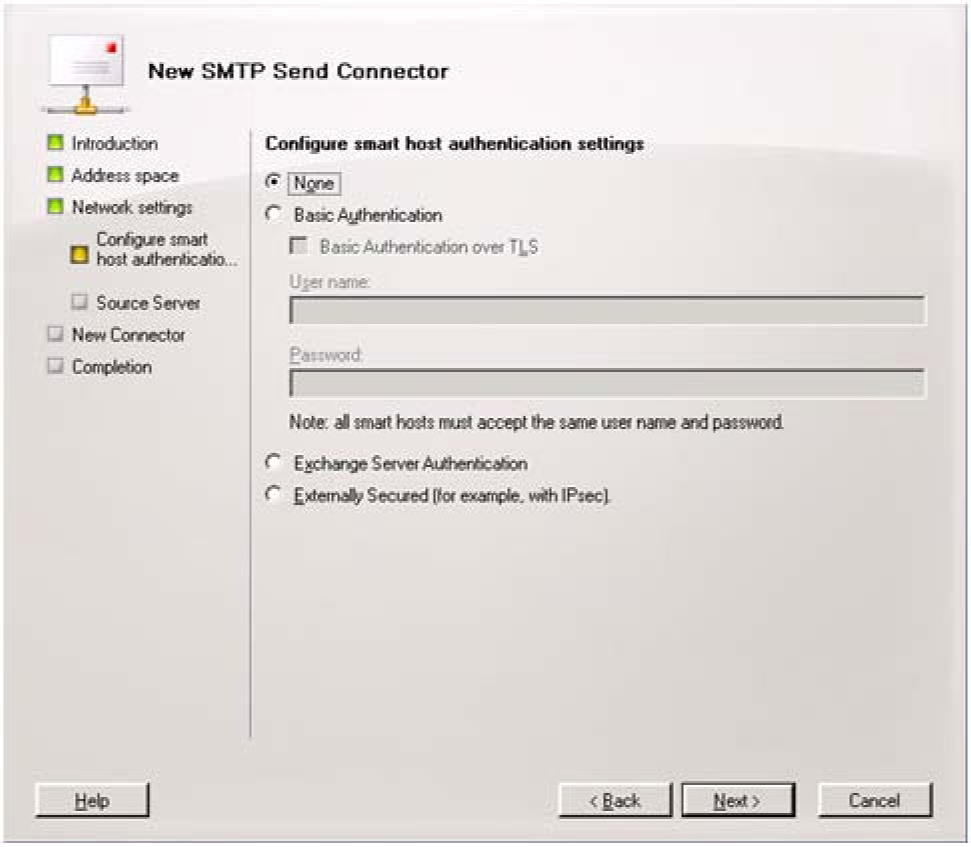
OK Cancel

□ Use the External DNS Lookup settings on the transport server

11. On the Configure smart host authentication settings page, make sure that the None radio button is selected, and click Next. You do not need SMTP authentication to send journal messages to the RazorSafe.

If you want a secure communication between Exchange and the RazorSafe appliance, you must configure Exchange to send journal messages to a mailbox. For more information, see Creating and Enabling Journal Rules in Exchange 2007/2010 on page 29 (step 5).

Figure 16 New SMTP Send Connection - Configure Smart Host Authentication Settings



Configure smart host authentication settings

● None

○ Basic Authentication

□ Basic Authentication over TLS

User name:

Password:

Note: all smart hosts must accept the same user name and password.

○ Exchange Server Authentication

○ Externally Secured (for example, with IPsec)

12. On the Source Server page, accept the default, and click Next.
13. On the last page, summary information is displayed. Click New, then complete any additional configuration options and verify that the RazorSafe is accepting messages. For more information, see Additional RazorSafe Configuration Options on page 45 and Verifying RazorSafe Message Archiving on page 47.

Next Steps, Completing the RazorSafe Configuration

Once you have enabled journaling on Exchange, you must complete the configuration on the RazorSafe.

If you are running Exchange 2000/2003, you must create a POP or IMAP fetcher on the RazorSafe in order to complete the configuration. For more information, see Finishing the RazorSafe Configuration on page 43.

If you are running Exchange 2007/2010, and are sending journal messages to a valid, enabled mailbox (see Creating and Enabling Journal Rules in Exchange 2007/2010 on page 29, step 5), you must create an IMAP fetcher in order to complete the configuration. For more information, see Finishing the RazorSafe Configuration on page 43.

If you are running Exchange 2007/2010, and are sending journal messages to a mailbox-enabled contact (see Creating and Enabling Journal Rules in Exchange 2007/2010 on page 29, step 5), you do not need to configure an IMAP fetcher and can proceed to configure additional options on the RazorSafe and verify the overall deployment. For more information, see Additional RazorSafe Configuration Options on page 45 and Verifying RazorSafe Message Archiving on page 47.

4

Configuring IBM Lotus Domino for RazorSafe Archiving

This chapter includes procedural steps on how to configure an IBM Lotus Domino Server for RazorSafe archiving.

Understanding Journaling on Lotus Domino

Mail journaling allows Lotus Domino to capture a copy of specified messages a router processes. Journaling can capture all messages handled by the router or only messages that meet a defined criteria. Journaling is configured by specifying the Mail Journal that will receive journaled messages, then creating a Server Mail Rule(s) to specify which messages are sent to that Mail Journal.

Prior to configuring the RazorSafe, Mirapoint highly recommends reading the IBM product documentation on mail journaling and configuring system mail rules. You can find this information on the IBM Information Center and Support Portal:

Mail Journaling
Configuring System Mail Rules and Mail Journaling

Enabling Journaling on Lotus Domino

This section provides procedural information on how to enable journaling on Lotus Domino server.

System Requirements

Mail Journaling can be configured on any Lotus Domino server Release 5 and higher. However, Mirapoint only supports Lotus Domino server Release 7 and higher. For more information about IBM end-of-support dates and products, see the IBM Support Portal.

Enabling Journaling in Lotus Domino

To properly set up Mail Journaling on Lotus Domino, you must complete the following steps:

1. Set up the Mail Journaling database.
2. Create Server Mail Rules to specify which messages to journal.

The following procedure provides an example of how to configure Mail Journaling. Mirapoint highly recommends that you follow the instructions in the Lotus Domino Administrator Help for your specific release. The Administrator Help can be found on your Lotus Domino server, in the help folder, using your Lotus Notes client. Within the Administrator Help, search for `Mail Journaling`.

To enable journaling:

The following steps assume that you are enabling Mail Journaling for a domain with one or more Lotus Domino servers. Also, specific steps refer you to the IBM Lotus Domino and Notes Information Center for Lotus Domino Release 8.5 and 8.5.1, but this information is applicable to earlier releases.

1. Create a RazorSafe user in Lotus Domino. This is the user that RazorSafe will use to fetch emails from the Mail Journal. This user must use POP3 to access the mail file, pull the message to the RazorSafe, and remove the message from the Mail Journal. The mail file for this user will be the Mail Journaling database (i.e., the mail-in database referred to in step 2b).

   Register the RazorSafe user in the Domino Directory. Mirapoint recommends using these settings:

   Use last name, `RazorSafe`, with no first name.

   Use `mail\razorsafe.nsf` as the name of the mail database.

   Use the standard mail template for your organization.

   Be sure to use a strong Internet password. The name and Internet password are used later when you configure RazorSafe to use POP3 to access the Mail Journal.

2. Set up the Mail Journaling database.

   For detailed procedural information on how to configure this database, see Setting up the Mail Journaling database in the Lotus Domino Administrator Help.

   a. In the Domino Directory, edit the Configurations Settings document for the server that you wish to configure Mail Journaling for. You must have a Configurations Settings document for each mail server using Mail Journaling.

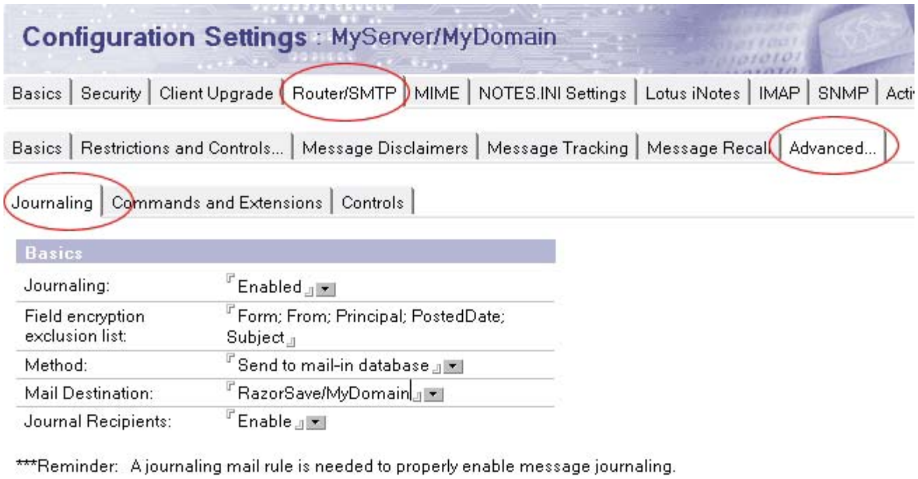
      If a Configurations Settings document does not exist for the server, you must create one.

b. The following example (Configuration Settings (Example) - Journaling Tab) shows a Configurations Settings document for `MyServer/MyDomain`. Mirapoint recommends using the Send to mail-in database method because it allows your organization to configure all mail servers to send Mail Journaling to one central mail database on one server.

Go to Router/SMTP > Advanced... > Journaling and complete the fields using the Configuration Settings (Example) - Journaling Tab as a guide.

For the Mail Destination field, make sure that you select the RazorSafe user you created in step 1.

Figure 17 Configuration Settings (Example) - Journaling Tab



Configuration Settings : MyServer/MyDomain
Basics | Security | Client Upgrade | Router/SMTP | MIME | NOTES.INI Settings | Lotus iNotes | IMAP | SNMP | Acti
Basics | Restrictions and Controls... | Message Disclaimers | Message Tracking | Message Recall | Advanced... |
Journaling | Commands and Extensions | Controls |
Basics

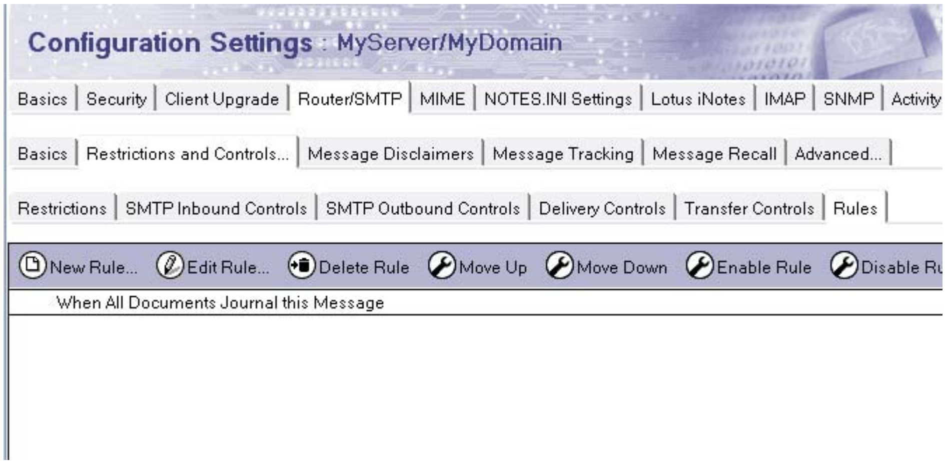
Journaling:	Enabled
Field encryption exclusion list:	Form; From; Principal; PostedDate; Subject
Method:	Send to mail-in database
Mail Destination:	RazorSave/MyDomain
Journal Recipients:	Enable

***Reminder: A journaling mail rule is needed to properly enable message journaling.

3. Create a Server Mail Rule that will send messages to the Mail Journal. Edit the Configurations Settings document for the mail server:

a. Go to Router/SMTP > Restrictions and Controls... > Rules.

Figure 18 Configuration Settings - Rules Tab



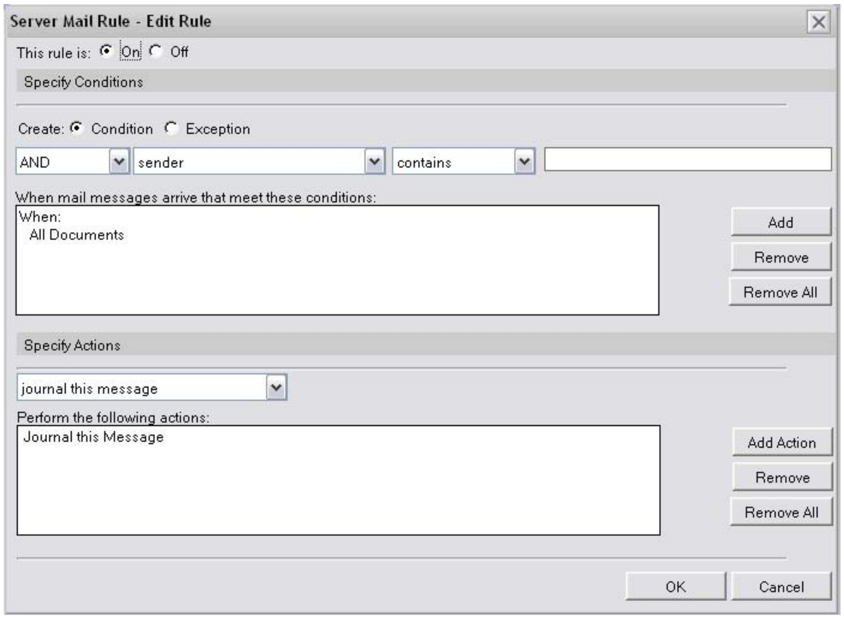
Configuration Settings : MyServer/MyDomain
Basics | Security | Client Upgrade | Router/SMTP | MIME | NOTES.INI Settings | Lotus iNotes | IMAP | SNMP | Activity
Basics | Restrictions and Controls... | Message Disclaimers | Message Tracking | Message Recall | Advanced... |
Restrictions | SMTP Inbound Controls | SMTP Outbound Controls | Delivery Controls | Transfer Controls | Rules |
New Rule... Edit Rule... Delete Rule Move Up Move Down Enable Rule Disable Ru

When All Documents Journal this Message

b. On the Rules tab, click New Rule....

c. Create a new rule for All Documents that uses the journal this message action (see Figure 19). For more information on rules, see Setting server mail rules in the Lotus Domino Administrator Help.

Figure 19 Server Mail Rule (Example)



Server Mail Rule - Edit Rule

This rule is: ● On ○ Off

Specify Conditions

Create: ● Condition ○ Exception

AND | sender | contains

When mail messages arrive that meet these conditions:

When:
All Documents

Specify Actions

journal this message

Perform the following actions:

Journal this Message

d. Click OK.

e. Click Save & Close.

4. (Optional) Depending on your Lotus Domino server release, you might need to restart the server.

For more feature information and troubleshooting information regarding Lotus Domino and RazorSafe, see Frequently Asked Questions on page 53.

Next Steps, Completing the RazorSafe Configuration

Once you have enabled journaling on Lotus Domino, you must complete the configuration on the RazorSafe. For more information, see Completing the RazorSafe Configuration on page 43.

5

Completing the RazorSafe Configuration

This chapter provides procedural steps on how to configure RazorSafe to work with a supported and configured email server (e.g., Mirapoint Message Server, Microsoft Exchange Server, etc.) using the RazorSafe administration interface.

Finishing the RazorSafe Configuration

To complete the RazorSafe configuration, complete the following steps:

1. Log in to the RazorSafe administration interface using the default GUI administration account and password (the default is `admin` and `ChangeMe` respectively).
2. Be sure to complete the following steps prior to configuring the appliance for email fetching:
   a. Click the Configuration tab.
   b. Under the Registration section on the left menu bar, click Register Product and complete the registration procedure.
   c. Under the System Settings section on the left menu bar, click Set Date/Time and set the appliance’s proper date and time.
   d. Under the System Setting section on the left menu bar, click Email Settings and set the default character set and email storage scheme.

> Once email data begins to be stored on the appliance this configuration option cannot be changed.

   e. Under the Network Settings section on the left menu bar, click Email Notification and set the administrator email address and delivery method. A daily email report is sent to the specified administrator detailing the status of the appliance.
   f. Click the Maintenance tab.

g. Under the Product Updates section on the left menu bar, click Upgrade Now and upgrade the appliance, if necessary.

For more information on any of these configuration steps, see the RazorSafe online help.

3. (For Mirapoint S7000-RS Appliances Only) If you have not already done so, make sure you have properly set up and configured your SAN storage device. For more information, see Configuring SAN Storage on page 49.

4. Set up the RazorSafe to get email from the email server by completing the following steps:

a. Click the Configuration tab.

b. Under the Email Servers section on the left menu bar, click POP or IMAP Fetchers.

The Email Server Configurations page appears.

c. Type in the name of the server in the text field, then click Add Server. The Fetcher Configuration page appears.

d. Populate the following fields as indicated in Table 6, then click Create Fetcher.

Table 6 RazorSafe New Email Server Parameters

New Server Configuration Fields	Value Description
Configuration Name	A description of the configuration, (for example, `Mirapoint Archive`).
Server Address	The fully-qualified domain name (FQDN) of the Message Server you are configuring (for example, `example.com`) or the IP address.
Server Description	A description of the email server you are setting up (for example, `Archive example.com email`).
User Name	The username you created to manage this server (for example, `journalmailbox`).
Password	A password you created for the username.
Activate Email Server	Select this checkbox to activate the server.
Server Protocol	Select an email server type (i.e., IMAP4, POP3, etc.) from the drop-down menu. The sIMAP4 and sPOP3 options represent the secure (SSL) versions of the POP3 and IMAP4 protocols.
Port Number	Select a port number for the selected email server protocol. For example, the default port number for POP3 is 110.

Table 6 RazorSafe New Email Server Parameters

New Server Configuration Fields	Value Description
Mailbox Name	Type in the mailbox you are fetching from. The default is `inbox`. If you want to fetch from a mailbox besides the inbox, you must use IMAP rather than POP. POP3 is only capable of connecting to the inbox.
Create Additional Archive Mailboxes	(This setting applies to Mirapoint Message Server appliances only.) Selecting this checkbox will create a set of 7 fetchers by appending 01 through 07 to the username you specified.
Email Deletion	Select one of the following radio buttons: Delete Emails Once Archived (More Secure) - This option is selected by default. Delete Emails Immediately (Faster)
Fetch Timeout	Type in the maximum number of minutes an email should be allowed to download. The default is 15 minutes. If a message takes longer than the maximum time, it will be recorded as a download failure and reported in the nightly email.

5. Test your email server configuration by completing the following steps:

   a. Under the Email Servers section on the left menu bar click, POP or IMAP Fetchers.

      The Email Server Configurations page appears.

   b. From the list of configurations, click the test icon (✓) for the email server you configured in step 4.

   If you get an error message, you have not configured your email server properly.

   Click the edit icon (✏) for the email server you just tested to open the Edit Fetcher Configuration page. Make the necessary corrections, click Submit, then return to the Email Server Configurations page to retest the configuration.

Additional RazorSafe Configuration Options

In addition to configuring the RazorSafe to work with an email server, you must create user accounts for anyone who will need to access the archived emails. This can be done manually or using LDAP/Microsoft Active Directory support. You add and configure these user accounts using options within the Users and Groups tab of the administration interface. For more information on LDAP/Active Directory support, see Setting Up RazorSafe for LDAP/Microsoft Active Directory Authentication on page 46.

After you have added user accounts, also make sure that you set the following options on the appliance. All of these options are available on the Configuration tab:

Proxy Server Setup

SMTP Server

IP Access Control

EncrypTape(R) Setup

Scheduled Searches

Remote Backup Schedule

Data Retention Policy

For more information on POP or IMAP Fetchers and archive scheduling, see Expanding Message Storage Capacity for Mirapoint Message Servers on page 59 and Using RazorSafe Backup and Restore on page 49, respectively. For more information on all of these features, see the RazorSafe online help.

If you have not already done so, Mirapoint recommends reading through the Mirapoint Support Knowledge Base, accessible from the Mirapoint Support website, for additional RazorSafe information.

Setting Up RazorSafe for LDAP/Microsoft Active Directory Authentication

Many companies use organizational units (OUs) to organize their Active Directory user accounts and objects. Companies also set up OUs by location or department. In RazorSafe, an authenticator treats an OU as a group. So, all rights assigned to an authenticator will apply to those user objects contained within the OU that you configure the LDAP connector to use.

For example, if you have an OU named `Central Office`, create an authenticator for that OU, and assign Email Viewing > Search permissions to that authenticator, then all user objects within `Central Office` will only have the capability of searching on their own email accounts.

Within RazorSafe you can add LDAP User Authenticators to authenticate against OUs that store user account objects. You create an LDAP User Authenticator using the LDAP Authenticator Wizard.

To access the LDAP Authenticator Wizard from the RazorSafe administration interface:

1. Click the Users and Groups tab.
2. Under the Alternate Authentication section on the left menu bar, click LDAP/ Active Directory.

   The LDAP User Authenticators page appears.
3. Type in a name for the authenticator in the text field and click Add Auth.

The LDAP Authenticator Wizard appears. The initial page of the wizard asks you to provide a Configuration Name and select a Server Type.

The Microsoft Active Directory, Mirapoint LDAP, and Novell eDirectory (GroupWise) server types are fully verified to work with the RazorSafe. If you are using a different LDAP server type, make sure that you select Open LDAP/Other LDAP as the Server Type and ensure that the defaults set within the wizard are correct. These defaults vary greatly based on the server type.

For more information on LDAP User Authenticators and the LDAP Authenticator Wizard, Mirapoint recommends reading the RazorSafe online help.

Verifying RazorSafe Message Archiving

After the setup of the email server and RazorSafe, you can verify that messages are downloading successfully to the RazorSafe appliance by using the administration interface.

Within the interface, click the Email Viewing tab, then navigate to Viewers > All Emails on the left menu bar to check the message count on any given day. You can also go to Viewers > Summary Counts, to view the email summary counts for all messages stored on the appliance. Once the messages are indexed, you can use the search features under the Searching section on the left menu bar to look for emails and verify that messages are being downloaded successfully.

Installing and Using Email Client Tools

After completely configuring the RazorSafe, make sure that the appropriate users install any necessary client tools for your environment.

To download client tools from the RazorSafe administration interface:

1. Click the Maintenance tab.
2. Under the Additional Features section on the left menu bar, click Download Tools.

   The Download Tools page appears. Clicking the link will lead you to an update page where you can download the latest version of the client tools.

For information about the various client software tools, see the Client Software documentation for your AOS release, available on the Mirapoint Support website.

A

Using RazorSafe Backup and Restore

This appendix includes procedural steps on how to backup and restore appliance data using a remote server (i.e., NFS or CIFS/SMB), as well as how to backup and restore emails.

Using Remote Backup and Restore

Remote Backup is used to do full and incremental backups to a device located elsewhere on the network. This backup can be used to restore the RazorSafe to its previous state in the event of a catastrophic failure.

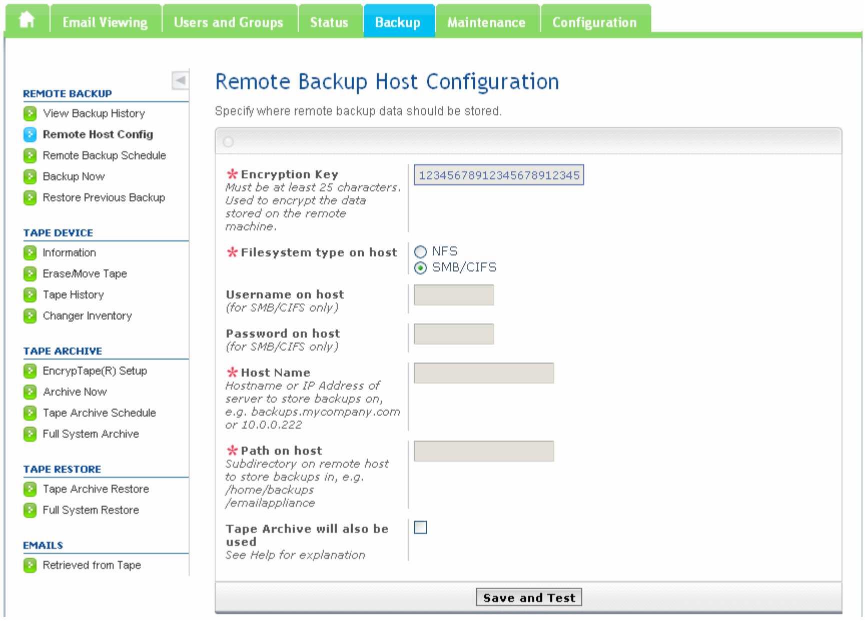
Remote Backup provides the highest speed of recovery in a system recovery scenario and also allows centralization of backup policies, procedures, and tools.

Performing a Backup on to a Remote Host

To back up your RazorSafe on to a remote host, complete the following steps:

1. Click the Backup tab.
2. Under the Remote Backup section on the left menu bar, click Remote Host Config.

Figure 20 Remote Backup Host Configuration



Remote Backup Host Configuration

Specify where remote backup data should be stored.

*Encryption Key Must be at least 25 characters. Used to encrypt the data stored on the remote machine.	12345678912345678912345
*Filesystem type on host	○ NFS ● SMB/CIFS
Username on host (for SMB/CIFS only)	
Password on host (for SMB/CIFS only)	
*Host Name Hostname or IP Address of server to store backups on, e.g. backups.mycompany.com or 10.0.0.222	
*Path on host Subdirectory on remote host to store backups in, e.g. /home/backups /emailappliance	
Tape Archive will also be used See Help for explanation	□

3. Type in an Encryption Key into the text field - This is a security feature to scramble the data that is backed up on the remote host. The key must be at least 25 characters long.

   Once the key is set, it should not be changed, because incremental backups are not allowed in the same host/directory if the encryption key does not match. If the backup needs to be restored onto a replacement unit, the replacement unit must be configured with the same host/directory and the same encryption key in order to access the remotely backed-up data.

4. Select one of the following Filesystem type on host radio buttons:

   NFS - Network File System, which is available on most UNIX, AIX, Linux, and Solaris servers.

   SMB/CIFS - Server Message Block protocol/Common Internet File System, which is available on Windows-based servers. If you selecting this filesystem type, type in the appropriate information for the Username on host and Password on host text fields that appear. This username and password pair is be used to authenticate the network connection. For more information, see Setting up a SMB/CIFS share on a Microsoft Windows XP Host on page 51.

5. Type in a Host Name in the text field - The hostname or IP address of the server that will host the backup (that is, providing the storage space). For example, `backups.mycompany.com`, or `10.0.0.222`, or `hostnameOfPC`.

6. Type in a Path on host in the text field - This is the directory path on the host server where the backups are stored. It should start with a forward slash (/) and use forward slashes (/) to separate further subdirectory names. For SMB/CIFS, the first subdirectory name of the path should be the Share name as it appears on the network, e.g., `/sharedemailbackups`. For more information, see Setting up a SMB/CIFS share on a Microsoft Windows XP Host on page 51.

7. Click Save and Test.

Changes are saved even if the connection to the remote host failed. In order for remote backups to succeed, the remote host must be accessible. Take note of any error messages that are displayed and make corrections accordingly.

By default backups occur daily at 17:00. You can also specify a backup schedule on the Remote Backup Schedule page. For more information, see the RazorSafe online help.

8. (Optional) After configuring your remote host, you can backup the RazorSafe immediately by completing the following steps:
   a. On the Backup tab, under the Remote Backup section, click Backup Now.
   b. Click Begin Backup.

Setting up a SMB/CIFS share on a Microsoft Windows XP Host

This section provides procedural steps on how to set up a SMB/CIFS share on a Microsoft Windows XP host. This procedure might differ on other Windows versions. For more information, see your Microsoft Windows product documentation.

To set up a SMB/CIFS share on Windows XP:

1. Create a user account:
   a. Go to the Windows Start menu and select Control Panel.
   b. Double-click on User Accounts.
   c. Select the Advanced tab and click Advanced.
   d. Right-click on the Users folder and select New User....
   e. Type in the appropriate information for all of the fields (e.g., User name, Password, etc.)
   f. Click Create.

Limit username and password lengths to 8 chars to avoid `mount error 11` issues.

2. Create a shared folder:
    a. Go to the Windows Start menu and select My Computer.
    b. Double-click on one of your drives (e.g., `C:\`).
    c. Click Make a new folder (e.g., `C:\emailbackups\`).
    d. Right-click on the folder and select Sharing and Security....
    e. On the Sharing tab, select the Share this folder radio button.
    f. Type in a Share name in the text field. (e.g. `sharedemailbackups`).

    You will need this name when configuring Remote Backup on the RazorSafe. For more information, see Performing a Backup on to a Remote Host on page 49.

    g. Click Permissions.
    h. Select Everyone and click Remove.
    i. Click Add... and type in the information for the user account you created in step 1 (e.g., `hostnameOfPC\username`).
    j. Select the Allow checkboxes for Change and Read permissions.
    k. Click OK.
    l. On the folder's Properties window, click OK.

Performing a Restore from a Remote Host

This procedure will restore previously backed up data from the location specified on the Remote Backup Host Configuration page (Backup > Remote Backup > Remote Host Config). Restoring from a remote host is generally used for system recovery.

Restoring from a remote host will wipe all existing data. Therefore, a restore can only be performed on a replacement appliance or a secure data wiped appliance. For more information on Secure Data Wipe functionality (Maintenance > Erase > Secure Data Wipe), see the RazorSafe online help.

The encryption key on the appliance (specified on the Remote Backup Host Configuration page) must exactly match the encryption key on the unit that the backup originated from.

To restore from a remote host, complete the following steps:

1. Click the Backup tab.
2. Under the Remote Backup section on the left menu bar, click Restore Previous Backup.
3. Click Begin Restoration.
4. (Optional) If you want to be notified by email when the rebuild completes, type a valid email address in the Email Address text field.
5. Click Begin Restore to begin the rebuild.

B

Performing a System Recovery of a RazorSafe Appliance

This appendix includes procedural steps on how to reinstall the Archive Operating System (AOS) from a System Recovery CD before performing a full restore of your entire RazorSafe appliance from recent backups.

Identifying the Appliance's Problem

Because system recovery is a last resort, try to identify the problem with the appliance to determine if a system recovery can be avoided:

1. Check your RazorSafe appliance's reports (i.e., system status, full system help checkup report, etc.) and logs (i.e., audit log, diagnostic log) for messages that might indicate what caused the problem.
2. To help identify hardware problems, see the Troubleshooting section of the hardware manual for your appliance model.
3. For a hardware failure of any kind, contact Mirapoint Technical Support for assistance. The failure might have been caused by power or wiring problems that can be corrected without system recovery.

The appliance does not back up the following information, so you need to record it:

Interface: The network interface, eth0 or eth1, depending on which ethernet port is connected to the LAN.

IP Address: The public Internet Protocol (IP) address assigned to the appliance, in dotted-quad notation (such as 10.1.1.1).

Netmask: The network class for computers on the same subnet as the appliance, in dotted-quad notation (such as 255.255.255.0).

Default Gateway: A computer or network that allows or controls access to another computer or network.

Fully-Qualified Domain Name (FQDN): The unique specification of the hostname and the complete domain name.

DNS Server (i.e., Nameserver): A program or server that implements a name service protocol.

With RAID storage and hot spare, RazorSafe appliances can tolerate one disk failure before they run in degraded mode, and up to three disk failures before recovery is mandatory. Of course, quickly replacing any failed disk can avert appliance degradation or the need for recovery.

Recovery Prerequisites

Before recovering an appliance, you must have:

The appliance’s product key (or Maintenance Key/Serial Number). The key is accessible from Status > Reports > System Info within the RazorSafe administration interface. You need the key in order to complete the recovery procedure. If you have any issues with your product key, contact Mirapoint Technical Support.

The System Recovery CD containing Mirapoint AOS system software

The Mirapoint RazorSafe 7-Series Hardware Getting Started Guide for your appliance and the Mirapoint RazorSafe System Software Release Notes for the AOS release you were running before the system recovery.

A terminal or PC with a terminal emulator connected to the appliance’s console port

If recovering from disk failures, replacement disks to configure as a RAID array

A computer on the network that can have web browser access to the appliance

Reinstalling AOS from the System Recovery CD

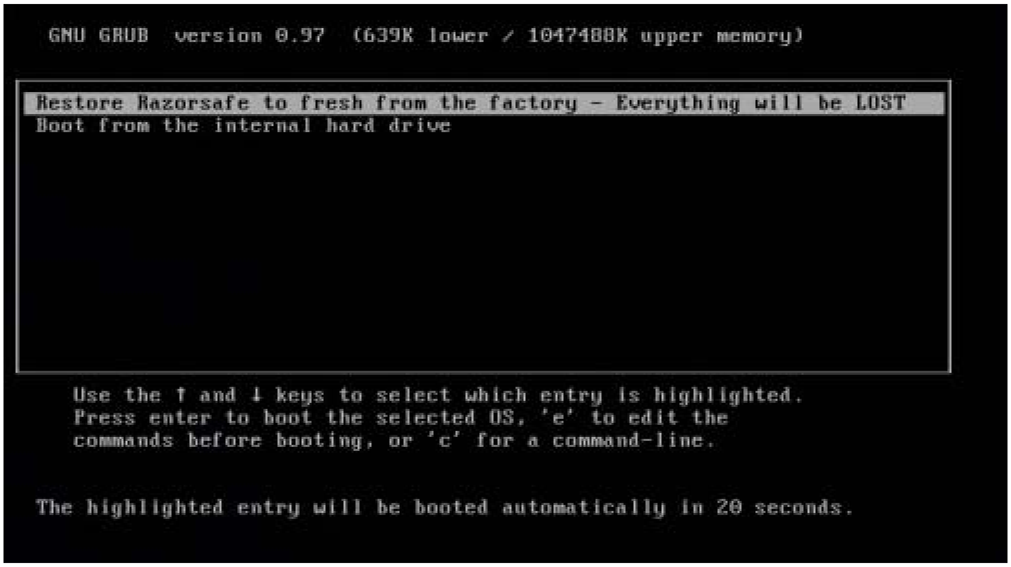
To reboot and reinstall AOS from a System Recovery CD:

1. Attach a console to the Mirapoint appliance.
2. Remove the front bezel from the appliance. For more information, see the Mirapoint RazorSafe 7-Series Hardware Getting Started Guide.
3. Insert the System Recovery CD into the appliance’s CD/DVD drive.
4. Boot the appliance from the System Recovery CD:

    If the appliance power is on, put the CD in the CD/DVD drive and reboot the appliance.

    If the appliance power is off, power on the appliance and then put the CD in the CD/DVD drive.

    After a few minutes of booting up, the console displays.



```
 GNU GRUB  version 0.97  (639K lower / 1047488K upper memory)

 Restore Razorsafe to fresh from the factory - Everything will be LOST
 Boot from the internal hard drive

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    commands before booting, or 'c' for a command-line.

 The highlighted entry will be booted automatically in 20 seconds.
```

5. Make sure that the `Restore Razorsafe to fresh from the factory - Everything will be LOST` option is selected and press `Enter`.

   The installation process will begin. After a few moments the following prompt will display:

   ```
   Is it okay to re-format the hard drive(s) [y/n]?
   ```

6. Type `y` and press `Enter`.

   The System Recovery CD erases all appliance data and reinstalls AOS on the appliance. This process might take a while to complete. Once complete, the console displays the following message:

   ```
   Installation is complete. Reboot now.
   ```

   Afterward, the appliance powers off.

7. Power on the appliance. When the console is blank, eject the System Recovery CD from the appliance.

8. After booting the console will display a message and prompt you for a login username. For example:

   ```
   This is razorsafe.unknown_domain (Linux x86_64 2.6.32.12) 05:56:01

   razorsafe login:
   ```

9. Type in the username: `enterkey`. For example:

   ```
   This is razorsafe.unknown_domain (Linux x86_64 2.6.32.12) 05:56:01

   razorsafe login: enterkey
   ```

10. You are prompted for the password. Type in the password: `enterkey`. For example:

    ```
    This is razorsafe.unknown_domain (Linux x86_64 2.6.32.12) 05:56:01

    razorsafe login: enterkey
    Password: enterkey
    ```

The console will not display the password text as you type.

After logging in, the following message is displayed and you are prompted to enter the for the product key. For example:

```
Your MAC address need for registering is:09:00:27:00:45:ac

To not enter the product key enter: quit
Please enter your product key:
```

11. Type in the key and press `Enter`.
12. After the product key is entered you are prompted to re-enter your RazorSafe login username and password. Type in your username as `miradmin` and password as `ChangeMe`. For example:

```
razorsafe login: miradmin
Password: ChangeMe
```

The password is case-sensitive

The Configuration Utility screen appears.

If you set up a static IP manually, instead of using DHCP, ensure that all fields are filled out correctly before confirming the changes. Any incorrect values will cause the appliance to be unreachable via the network. Static IP settings require that the following be specified:

Network Interface

IP Address

Netmask

Default Gateway

Full-Qualified Domain Name

DNS Server

For more information, see Assigning IP Addresses on page 13.

13. Log in to the web administration interface (i.e., `https://`*`IP_address_or_FQDN_of_appliance`*), using username `admin` and password `ChangeMe`.

The password is case-sensitive

14. Click on the Configuration tab, then select from the following navigation options in the order listed:

    a. Set Date/Time

    b. Email Settings

    c. Email Notification

For more information, see Finishing the RazorSafe Configuration on page 43.

Recovering the Appliance from Backup

Recovering the appliance from a backup as part of the system recovery process involves performing a restore. You can restore appliance data and emails from a remote host. For more information, see Using RazorSafe Backup and Restore on page 49.

When restoring data from a remote host backup, you can restore only to an appliance of the same hardware model (or higher), running the exact same AOS release as the backed up appliance.

C

Expanding Message Storage Capacity for Mirapoint Message Servers

Mirapoint Message Servers have a 150K message limitation in user folders. This limitation can cause problems for both the Message Server and RazorSafe when that threshold is exceeded. If messages are not moved from the user folder, they begin to queue and if their volume continues to increase, service interruptions may occur on either the Message Server or RazorSafe appliance.

If your Message Server has moderate message traffic (for example, a few thousand messages per hour), this threshold should not be exceeded, but if you have high volumes of message traffic, you might want to add additional POP or IMAP Fetchers on the RazorSafe and additional journal mailboxes on the Message Server.

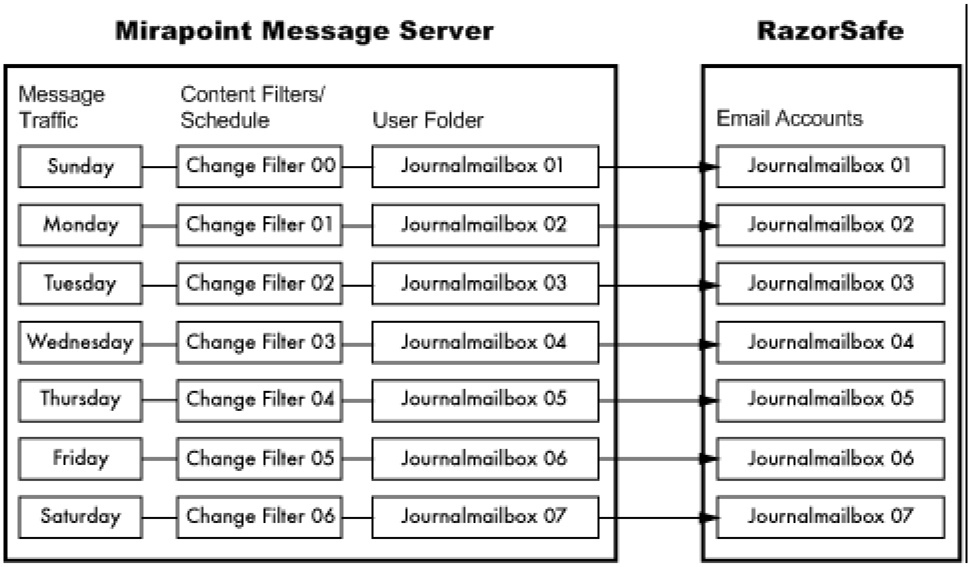
Process Overview

To increase the message storage capacity for your RazorSafe, you must create additional POP or IMAP Fetchers on the RazorSafe appliance and journal mailboxes on the Message Server. POP or IMAP Fetchers are server configurations set up to retrieve message copies from the journal mailboxes on the Message Server.

One option to increase message storage capacity is to create multiple POP or IMAP Fetchers on the RazorSafe appliance and to change the wiretap filter on a regular basis, thus expanding the total number of messages that can be stored awaiting archiving. For example, you could create seven accounts, one for each day of the week, and change the wiretap rule so messages are routed on a daily basis.

This is achieved by creating seven corresponding user folders on the Message Server; one for each day of the week (for example, `Journalmailbox 01` could be used for Sunday, `Journalmailbox 02` could be used for Monday). You then create seven schedules to change the wiretap filter so that the message copies are redirected to the appropriate user folder for whichever day it is (see Figure 21 below).

Figure 21 Expanding Storage Capacity: Day-of-the-Week Method



Configuration instructions for the day-of-the-week method of expanding your message storage capacity is described in detail in the sections that follow.

Setting Up Day-Of-The-Week Journaling

This section provides procedures on how to:

Create seven journal accounts on the RazorSafe (Adding Journal Accounts to a RazorSafe on page 60)

Create seven user folders on the Message Server (Setting Up a Mirapoint Message Server on page 62)

Delete the existing content filter and then add seven new content filters, one for each user folder.

Create seven new schedules, one for each content filter.

Adding Journal Accounts to a RazorSafe

To add journal accounts to a RazorSafe, complete the following steps:

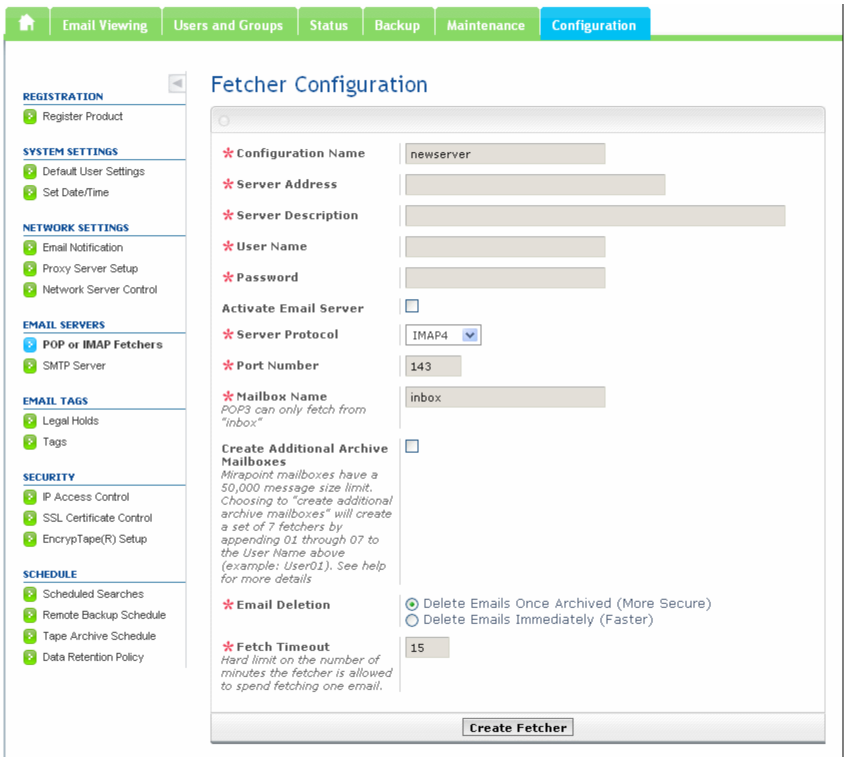
1. Open a web browser and navigate to the administration interface for the RazorSafe.
2. Login as an administrator. You can use the default username and password provided with your appliance (`admin` and `ChangeMe` respectively), unless you changed it.
3. Click the Configuration tab.
4. Under the Email Servers section on the left menu bar, click POP or IMAP Fetchers.

   The Email Server Configurations page appears.

5. Type in the name of the server in the text field, then click Add Server.

   The Fetcher Configuration page appears.

Figure 22 Fetcher Configuration Page with Create Additional Archive Mailboxes Checkbox



Fetcher Configuration

*Configuration Name	newserver
*Server Address	
*Server Description	
*User Name	
*Password	
Activate Email Server	□
*Server Protocol	IMAP4
*Port Number	143
*Mailbox Name *POP3 can only fetch from "inbox"*	inbox
Create Additional Archive Mailboxes *Mirapoint mailboxes have a 50,000 message size limit. Choosing to "create additional archive mailboxes" will create a set of 7 fetchers by appending 01 through 07 to the User Name above (example: User01). See help for more details*	□
*Email Deletion	● Delete Emails Once Archived (More Secure) ○ Delete Emails Immediately (Faster)
*Fetch Timeout *Hard limit on the number of minutes the fetcher is allowed to spend fetching one email.*	15

6. Populate the following fields as indicated in Table 7, then click Create Fetcher.

Table 7 RazorSafe New Fetcher Parameters

New Server Configuration Fields	Value Description
Configuration Name	A description of the configuration, (for example, `Mirapoint Archive`).
Server Address	The fully-qualified domain name (FQDN) of the Message Server you are configuring (for example, `example.com`).
Server Description	A description of the email server you are setting up (for example, `Archive example.com email`).
User Name	The username you created to manage this server (for example, `journalmailbox`).
Password	A password you created for the username.
Activate Email Server	Select this checkbox to activate the server.

Table 7 RazorSafe New Fetcher Parameters

New Server Configuration Fields	Value Description
Server Protocol	Select a the mail server type (i.e., IMAP4, POP3, etc.) from the drop-down menu. The sIMAP4 and sPOP3 options represent the secure (SSL) versions of the POP3 and IMAP4 protocols.
Port Number	Select a port number for the selected server protocol. For example, the default port number for POP3 is 110.
Mailbox Name	Type in the mailbox you are fetching from. The default is `inbox`. If you want to fetch from a mailbox besides the inbox, you must use IMAP rather than POP. POP3 is only capable of connecting to the inbox.
Create Additional Archive Mailboxes	Select this checkbox to create a set of 7 fetchers by appending 01 through 07 to the username you specified.
Email Deletion	Select one of the following radio buttons: Delete Emails Once Archived (More Secure) - This option is selected by default. Delete Emails Immediately (Faster)
Fetch Timeout	Type in the maximum number of minutes an email should be allowed to download. The default is 15 minutes. If a message takes longer than the maximum time, it will be recorded as a download failure and reported in the nightly email.

Setting Up a Mirapoint Message Server

You use the command-line interface (CLI) and Administration Protocol to setup your Message Server to use the day-of-the-week journaling method. This section provides procedures on how to:

Use the CLI to create seven new user folders and delete your old wire tap filter (Configuring Day-Of-The-Week Journaling with the CLI on page 63)

Use the administration protocol to create new filters and schedules to control the redirection of message copies to the new user folders (Creating Schedules Using the Administration Protocol on page 64)

Test your schedules and filters (Testing the Configuration on page 64)

Configuring Day-Of-The-Week Journaling with the CLI

1. Log in to the CLI as follows:

   a. Using a telnet client, connect to the default telnet port (port 23) on the Message Server. You can identify the appliance using the IP address you assigned to it.

   b. Log in as `Administrator` using the password you specified for the Message Server during its hardware setup. For example:

   ```
   OK mail.example.com admind 4.1 server ready

   User: Administrator
   Password: password
   OK User logged in
   mail.example.com
   ```

2. Using the `User Add` and `Mailbox Add` commands, create seven new user folders to be used as journal accounts on the Message Server. For example:

   ```
   User Add journalmailbox01 password “journalmailbox 01”

   Mailbox Add user.journalmaibox01

   User Add journalmailbox02 password “journalmailbox 02”

   Mailbox Add user.journalmaibox02

   User Add journalmailbox03 password “journalmailbox 03”

   Mailbox Add user.journalmaibox03

   User Add journalmailbox04 password “journalmailbox 04”

   Mailbox Add user.journalmaibox04

   User Add journalmailbox05 password “journalmailbox 05”

   Mailbox Add user.journalmaibox05

   User Add journalmailbox06 password “journalmailbox 06”

   Mailbox Add user.journalmaibox06

   User Add journalmailbox07 password “journalmailbox 07”

   Mailbox Add user.journalmaibox07
   ```

   In the example above, substitute *`journalmailbox01`* and the *`password`* with the corresponding username and password you created on the RazorSafe in Adding Journal Accounts to a RazorSafe on page 60.

3. Delete your current wiretap content filter using the following `Filter Delete` command:

   ```
   Filter Delete "RedirectAllEmail" Wiretap
   ```

4. Create a new filter to for the new user folders you created using the following command:

```
Filter Add "(domain=any)" "RedirectAllEmail" Wiretap "(to=journalmailbox01)" Allof
Continue ""
```

Creating Schedules Using the Administration Protocol

Create the seven new daily schedules by completing the following steps:

Do not create the schedules using the CLI.

1. Using a telnet client, log in to the Administration Protocol on port 10143. For example:

   ```
   Telnet mirapoint.example.com 10143
   ```

   ```
   tag Login Administrator Password
   ```

2. Create the seven new daily schedules using the `Schedule Add` command, for example:

```
tag Schedule Add ChangeFilter0 Weekly 0 ". Filter Change \"(domain=any)\"
\"RedirectAllEmail\" Wiretap \"(to=journalmailbox01)\" Allof Continue \"\""

tag Schedule Add ChangeFilter1 Weekly 1 ". Filter Change \"(domain=any)\"
\"RedirectAllEmail\" Wiretap \"(to=journalmailbox02)\" Allof Continue \"\""

tag Schedule Add ChangeFilter2 Weekly 2 ". Filter Change \"(domain=any)\"
\"RedirectAllEmail\" Wiretap \"(to=journalmailbox03)\" Allof Continue \"\""

tag Schedule Add ChangeFilter3 Weekly 3 ". Filter Change \"(domain=any)\"
\"RedirectAllEmail\" Wiretap \"(to=journalmailbox04)\" Allof Continue \"\""

tag Schedule Add ChangeFilter4 Weekly 4 ". Filter Change \"(domain=any)\"
\"RedirectAllEmail\" Wiretap \"(to=journalmailbox05)\" Allof Continue \"\""

tag Schedule Add ChangeFilter5 Weekly 5 ". Filter Change \"(domain=any)\"
\"RedirectAllEmail\" Wiretap \"(to=journalmailbox06)\" Allof Continue \"\""

tag Schedule Add ChangeFilter6 Weekly 6 ". Filter Change \"(domain=any)\"
\"RedirectAllEmail\" Wiretap \"(to=journalmailbox07)\" Allof Continue \"\""
```

The filter's name in the schedules above match the name of the existing filter, but the wiretap destination account is pointing at one of the accounts you created in step 2 on page 63.

Testing the Configuration

After you have added the new user folders and filter schedules, use the following CLI commands to verify you have correctly configured them.

```
User List
```

```
Schedule List
```

```
Filter Export (domain=any)
```

The `Filter Export` command lists all filters and their parameters configured on the Message Server.

You can verify the wiretap destination (for example, from *`journalmailbox03`* to *`journalmailbox04`*) at midnight on the day you make the change. Mirapoint also recommends adding your email address into the schedule-output distribution list, so that you can receive reports by the schedules you created.

For additional assistance on any of the steps detailed in this chapter, contact your Mirapoint Sales Engineer. In some cases, they can provide scripts to facilitate the configuration process.

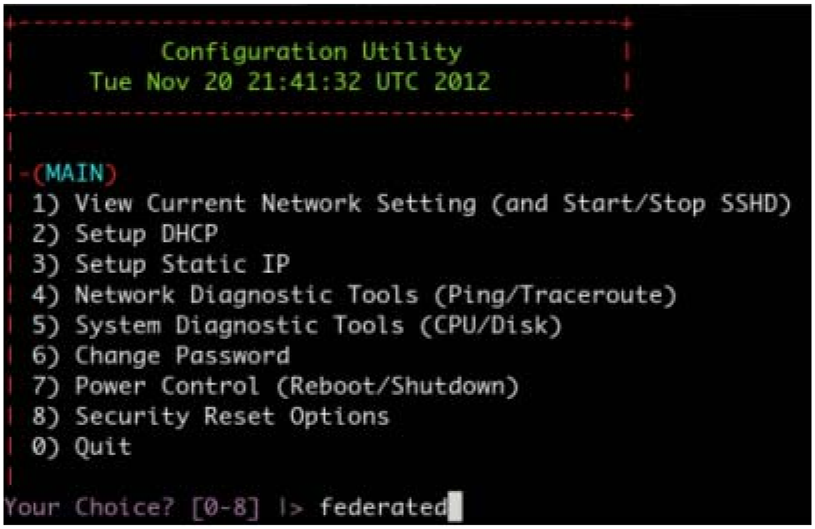
D

Federated Search

Federated search is a new feature that allows multiple machines to act as one while performing tasks such as searching. For example, two machines can be configured so that searching on one of the machines also runs a search on the other. These results are returned to the user on the machine where the search was made from. Any machine that will be used for federated search must be configured using its own acu command line utility for federated search.

Configuration

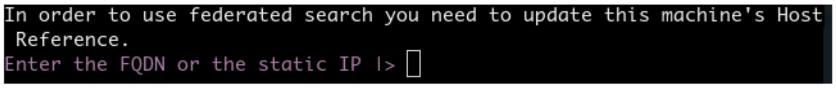
Configuration for federated search is performed through the acu command line. Federated search configuration should be performed when there are no users actively using the machine. Many of the options in the configuration will restart the search process, upon exiting the program, which will temporarily bring down the ability to perform searches.



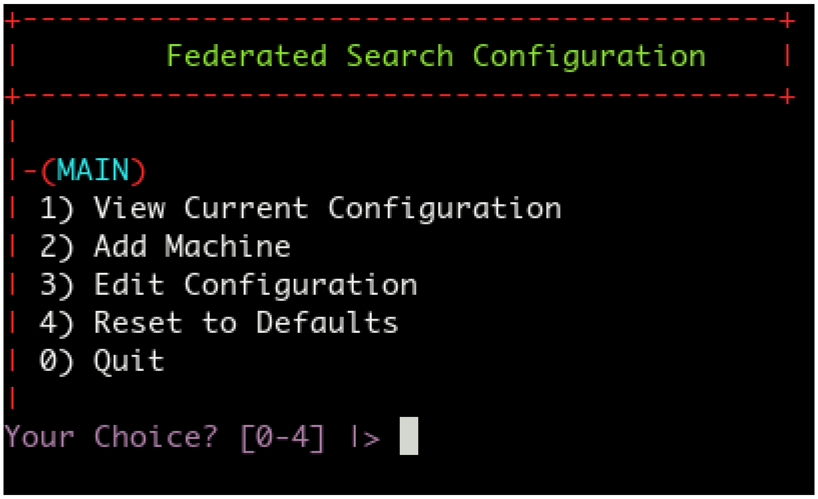
```
+------------------------------------------+
|          Configuration Utility           |
|     Tue Nov 20 21:41:32 UTC 2012         |
+------------------------------------------+
|
|-(MAIN)
| 1) View Current Network Setting (and Start/Stop SSHD)
| 2) Setup DHCP
| 3) Setup Static IP
| 4) Network Diagnostic Tools (Ping/Traceroute)
| 5) System Diagnostic Tools (CPU/Disk)
| 6) Change Password
| 7) Power Control (Reboot/Shutdown)
| 8) Security Reset Options
| 0) Quit
|
Your Choice? [0-8] |> federated
```

Access the Federated Configuration Utility by entering “federated” at the acu command line.

The first time the federated configuration utility is used it will ask for the current machine's Host Reference. The Host Reference is either the fully qualified domain name (FQDN) of the machine or the static IP address. This needs to stay consistent as it is the only way other boxes will be able to communicate with this machine.



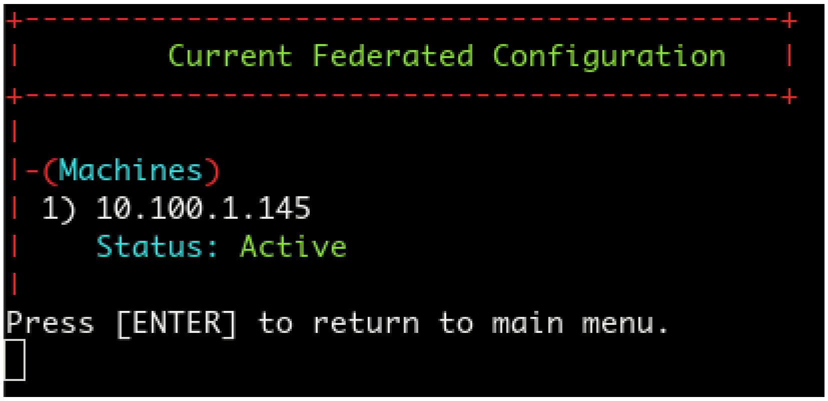
```
In order to use federated search you need to update this machine's Host
 Reference.
Enter the FQDN or the static IP |>
```



```
+-----------------------------------------+
|          Federated Search Configuration    |
+-----------------------------------------+
|
|-(MAIN)
| 1) View Current Configuration
| 2) Add Machine
| 3) Edit Configuration
| 4) Reset to Defaults
| 0) Quit
|
Your Choice? [0-4] |>
```

After entering the FQDN or static IP address the main configuration window will appear.

Entering 1 at the prompt will bring up the display for the current federated configuration.

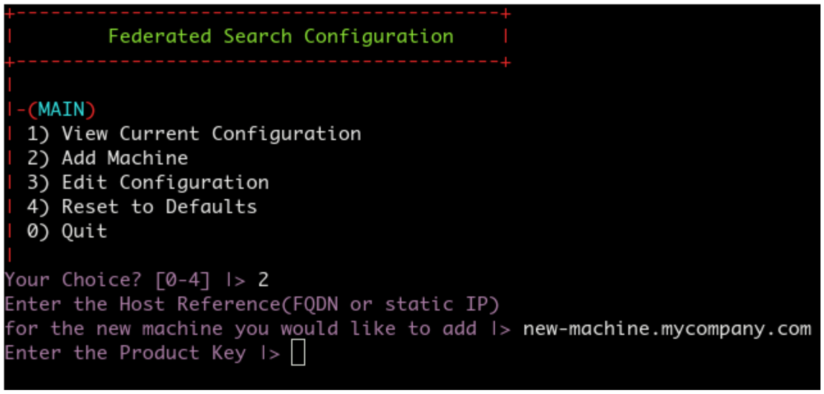


```
+-----------------------------------------+
|          Current Federated Configuration    |
+-----------------------------------------+
|
|-(Machines)
| 1) 10.100.1.145
|    Status: Active
|
Press [ENTER] to return to main menu.
```

This display shows which machines are actively connected to the current machine. Because no machines have been added to the configuration yet, only the current machine will show as being active.

Using the Add Machine option from the MAIN menu will prompt for the Host Reference for the new machine that is going to be added to the configuration. It will then prompt for the product key of the new machine. The new machine will automatically be activated in the configuration if successful.

The machine that is added also has to be configured through its own acu command line utility for federated search. The FQDN or static IP address entered in that configuration must match the information added in this configuration.



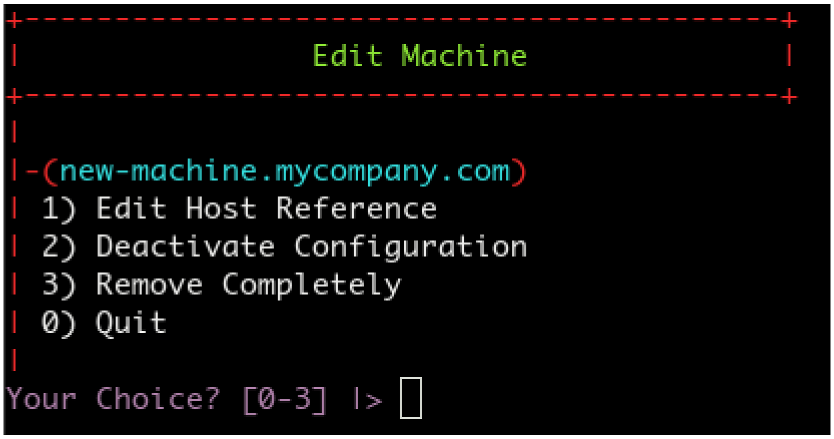
```
+-------------------------------------+
|       Federated Search Configuration    |
+-------------------------------------+
|
|-(MAIN)
| 1) View Current Configuration
| 2) Add Machine
| 3) Edit Configuration
| 4) Reset to Defaults
| 0) Quit
|
Your Choice? [0-4] |> 2
Enter the Host Reference(FQDN or static IP)
for the new machine you would like to add |> new-machine.mycompany.com
Enter the Product Key |>
```

The third menu “Edit Configuration” opens up the “Edit Federated Configuration” screen. Here a machine can be selected and then several options are presented at the “Edit Machine” screen. Here a user can edit the Host Reference for any machine, deactivate an activated machine, activate a deactivated machine, or remove the machine completely.

Activating a machine will make the current machine able to search on it.

Deactivating a machine will make the current machine unable to search on it.

Removing a machine will delete it's configuration from the current machine entirely.



```
+-------------------------------------------+
|                Edit Machine               |
+-------------------------------------------+
|
|-(new-machine.mycompany.com)
| 1) Edit Host Reference
| 2) Deactivate Configuration
| 3) Remove Completely
| 0) Quit
|
Your Choice? [0-3] |>
```

The fourth and final option from the MAIN menu is “Reset to Defaults”. This option deletes all of the current active or deactivated machines from the configuration and returns the settings to the way they were before federated search was configured.

Index

MIRAPOINT SOFTWARE, INC. SOFTWARE LICENSE AGREEMENT

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY BEFORE DOWNLOADING OR OTHERWISE USING THE SOFTWARE. BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS SOFTWARE LICENSE AGREEMENT.

IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, YOU ARE NOT AUTHORIZED TO DOWNLOAD OR USE THIS SOFTWARE.

1. Scope. This License governs you ("User") and your use of any and all computer software, any printed or electronic documentation, or other code, whether on disk, in read only memory, or on any other media (collectively, the "Mirapoint Software") provided to you as part of or with a Mirapoint Product.

2. License, not Sale, of Mirapoint Software. The Mirapoint Software is licensed, not sold, to User by MIRAPOINT SOFTWARE, INC. or its affiliate, if any ("Mirapoint"). USER MAY OWN THE MEDIA ON WHICH THE MIRAPOINT SOFTWARE IS PROVIDED, BUT MIRAPOINT AND/OR MIRAPOINT'S LICENSOR(S) RETAIN TITLE TO THE MIRAPOINT SOFTWARE. The Mirapoint Software installed on the Mirapoint Product and any copies which this License authorizes the User to make are subject to this License.

3. Permitted Uses. This License allows User to use the pre-installed Mirapoint Software exclusively on the Mirapoint Product on which the Mirapoint Software has been installed. With respect to Mirapoint Software [identified by Mirapoint as the "administrative application"] that has not been preinstalled on the Mirapoint Product, this License allows you to copy, use and install such Mirapoint Software on one or more administrative workstations on which the Mirapoint Software is supported. User may make copies of the Mirapoint Software in machine-readable form for backup purposes only, provided that such backup copy must include all copyright and other proprietary information and notices contained on the original.

4. Proprietary Rights; Restrictions on Use. User acknowledges and agrees that the Mirapoint Software is copyrighted and contains materials that are protected by copyright, trademark, trade secret and other laws and international treaty provisions relating to proprietary rights. User may not remove, deface or obscure any of Mirapoint's or its suppliers' proprietary rights notices on or in the Mirapoint Software or on output generated by the Mirapoint Software. Except as permitted by applicable law and this License, you may not copy, decompile, reverse engineer, disassemble, modify, rent, lease, loan, distribute, assign, transfer, or create derivative works from the Mirapoint Software. Your rights under this License will terminate automatically without notice from Mirapoint if you fail to comply with any term(s) of this License. User acknowledges and agrees that any unauthorized use, transfer, sublicensing or disclosure of the Mirapoint Software may cause irreparable injury to Mirapoint, and under such circumstances, Mirapoint shall be entitled to equitable relief, without posting bond or other security, including but not limited to, preliminary and permanent injunctive relief.

5. Third Party Programs. Mirapoint integrates third party software programs with the Mirapoint Software which are subject to their own license terms. These license terms can be viewed at http://www.mirapoint.com/licenses/thirdparty/eula.php. If User does not agree to abide by the applicable license terms for the integrated third party software programs, then you may not install the Mirapoint Software.

6. Disclaimer of Warranty on Mirapoint Software. User expressly acknowledges and agrees that use of the Mirapoint Software is at your sole risk. Unless Mirapoint otherwise provides an express warranty with respect to the Mirapoint Software, the Mirapoint Software is provided "AS IS" and without warranty of any kind and Mirapoint and Mirapoint's licensor(s) (for the purposes of provisions 5 and 6, Mirapoint and Mirapoint's licensor(s) shall be collectively referred to as "Mirapoint") EXPRESSLY DISCLAIM ALL WARRANTIES AND/OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN ADDITION, MIRAPOINT DOES NOT WARRANT THAT THE MIRAPOINT SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE MIRAPOINT SOFTWARE WILL RUN UNINTERRUPTED OR BE ERROR-FREE, OR THAT DEFECTS IN THE MIRAPOINT SOFTWARE WILL BE CORRECTED. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR OTHER DISCLAIMERS, SO THE ABOVE EXCLUSION OR DISCLAIMERS MAY NOT APPLY TO YOU.

7. Limitation of Liability. UNDER NO CIRCUMSTANCES, INCLUDING NEGLIGENCE, SHALL MIRAPOINT BE LIABLE FOR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO THIS LICENSE. FURTHER, IN NO EVENT SHALL MIRAPOINT'S LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF USE, DATA OR PROFITS OR INTERRUPTION), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (INCLUDING NEGLIGENCE OR OTHER TORT), ARISING IN ANY WAY OUT OF YOUR USE OF THE SOFTWARE OR THIS AGREEMENT, EVEN IF ADVISED OF THE POSSIBILITY OF DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THIS LIMITATION MAY NOT APPLY TO YOU. In no event shall

Mirapoint's total liability to you for all damages exceed the amount paid for this License to the Mirapoint Software.

8. Export Control. As required by the laws of the United States and other countries, User represents and warrants that it: (a) understands that the Mirapoint Software and its components may be subject to export controls under the U.S. Commerce Department's Export Administration Regulations ("EAR"); (b) is not located in a prohibited destination country under the EAR or U.S. sanctions regulations (currently Cuba, Iran, Iraq, North Korea, Sudan and Syria, subject to change as posted by the United States government); (c) will not export, re-export, or transfer the Mirapoint Software to any prohibited destination or persons or entities on the U.S. Bureau of Industry and Security Denied Parties List or Entity List, or the U.S. Office of Foreign Assets Control list of Specially Designated Nationals and Blocked Persons, or any similar lists maintained by other countries, without the necessary export license(s) or authorizations(s); (d) will not use or transfer the Mirapoint Software for use in connection with any nuclear, chemical or biological weapons, missile technology, or military end-uses where prohibited by an applicable arms embargo, unless authorized by the relevant government agency by regulation or specific license; (e) understands and agrees that if it is in the United States and exports or transfers the Mirapoint Software to eligible users, it will, to the extent required by EAR Section 740.17(e), submit semi-annual reports to the Commerce Department's Bureau of Industry and Security, which include the name and address (including country) of each transferee; and (f) understands that countries including the United States may restrict the import, use, or export of encryption products (which may include the Mirapoint Software and the components) and agrees that it shall be solely responsible for compliance with any such import, use, or export restrictions.

9. Miscellaneous. This License will be governed by and construed in accordance with the laws of the State of California, U.S.A., without reference to its conflict of law principles. If a court of competent jurisdiction finds any provision of this License invalid or unenforceable, that provision will be amended to achieve as nearly as possible the same economic effect as the original provision and the remainder of this License will remain in full force. Failure of a party to enforce any provision of this License shall not waive such provision or of the right to enforce such provision. This License sets forth the entire agreement between the parties with respect to your use of the Mirapoint Software and supersedes all prior or contemporaneous representations or understandings regarding such subject matter. No modification or amendment of this License will be binding unless in writing and signed by an authorized representative of Mirapoint. You will not export, re-export, divert, transfer or disclose, directly or indirectly, the Mirapoint Software, Mirapoint Products or any technical information and materials supplied under this Agreement without complying strictly with the export control laws and all legal requirements in the relevant jurisdiction, including without limitation, obtaining the prior approval of the U.S. Department of Commerce.